POSitivity magazine

THE OFFICIAL MAGAZINE OF MERCHANT PAYMENTS ECOSYSTEM • ISSUE 79 / MARCH 2019

mpe Merchant Payments Ecosystem

MPE 2019, Feb 19-21, Berlin

Key moments from conference chairs, speakers and press

MPE 2019 chair summaries

on page 6

MPE Awards 2019

on page 25

Articles by MPE 2019 Speakers

on page 40

Natalia Ivanis
Head of Marketing &
Media Partnership at Empiria Group

natalia.ivanis@merchantpaymentsecosystem.com

Welcome to the March Issue of POSitivity Magazine!

You are reading the post-conference Issue dedicated to MPE 2019 (Merchant Payments Ecosystem) conference and exhibition, that was held from February 19 – 21, in Berlin.

Before you dive into the reading about MPE'S key moments, I would like to mention few interesting milestones and facts about 12th edition of MPE conference:

MPE 2019 got over its magic threshold of participants this year. The number of participants exceeded 1,000+ industry professionals from 40+ countries.

MPE 2019 has also become the European event with the biggest merchant presence; it attracted this year the record number of 250 merchants from various merchant categories.

During three days of the event we have seen insights from over 140 industry leaders and influencers. The program was running in four conference rooms discussing the most pressing topics that are facing the industry.

In this Issue you will further read about some of the most important themes from this year's event along with highlights from the conference chairs, speakers and insights by the community members of the merchant payments ecosystem.

Attendees of the MPE 2019 event walked away with a ton of knowledge when it comes to the future of the merchant payments and financial industry as a whole.

In summing up this year's event, we believe that David Birch, said it best:
"Once again the Merchant Payments Ecosystem Conference in Berlin turned out to be an absolute must-attend event for everyone in our industry".

Enjoy the reading!

If you have any questions or comments, or if you are interested in contribution or Advertisement, please contact the POSitivity Magazine editor:
Ondrej Dorcik
ondrej.dorcik@merchantpaymentsecosystem.com

MPE 2019 SUMMARY

12th edition of “Merchant Payments Ecosystem” (MPE 2019) conference and exhibition

FEB 19-21 IN BERLIN WAS A HUGE SUCCESS!

Key Milestones and Facts:

- MPE 2019 get over its magic threshold of **THOUSAND** participants.
- MPE 2019 is the **BIGGEST EUROPEAN PAYMENT ACCEPTANCE EVENT.**
- MPE 2019 gathered **ENTIRE PAYMENT ECOSYSTEM**: merchants, acquirers, PSPs and Point of Sale vendors, established companies as well as start-ups, fintech, regtech and paytech and everyone in between.

WHAT WAS NEW @ MPE 2019?

MPE 2019 is the European event with the

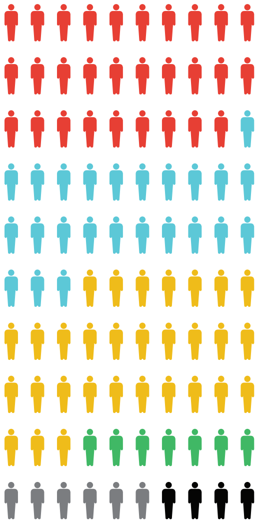
BIGGEST MERCHANT PRESENCE

it attracted this year the record number of **245 merchants** from various merchant categories.

WHO ATTENDED MPE 2019?

Europe's Largest Merchant Payment Conference
at glance:

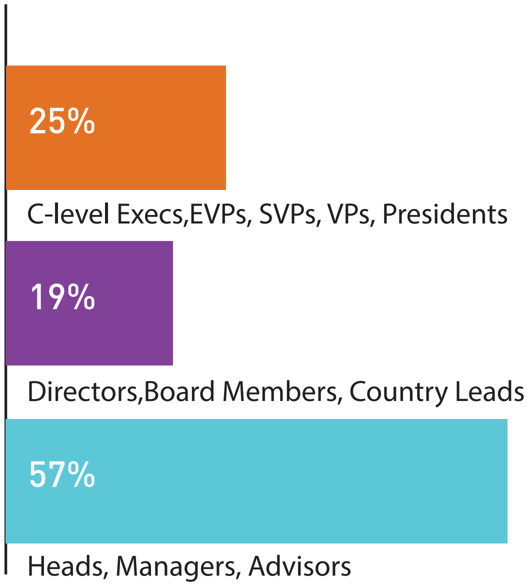
Industry breakdown



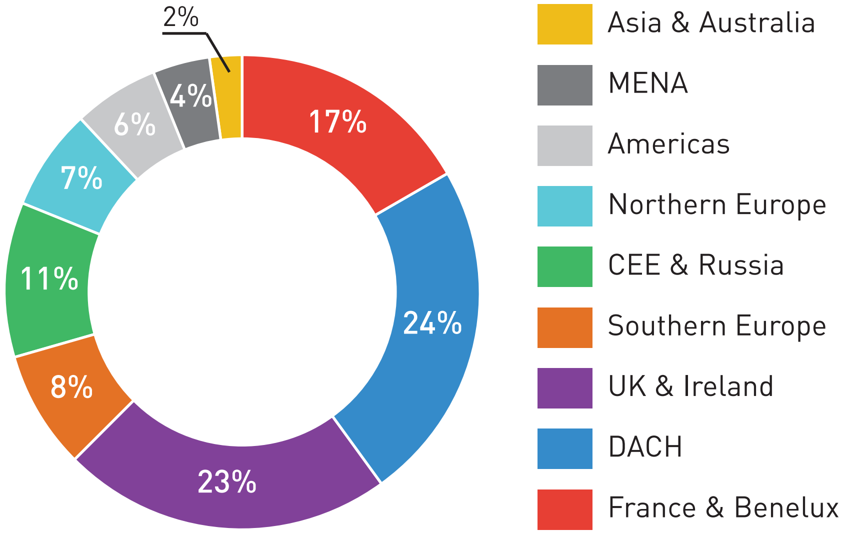
29%	Acquirers & PSPs
24%	Merchants
30%	Payment/Solution provider
7%	Regulator/Scheme/MNO/
6%	Industry Experts
4%	Other

1080 attendees, including **245** merchants and **300** acquiring banks & PSPs networked in a cozy atmosphere of the 5-star hotel and got inspiration from **140** TOP industry speakers, **75** solution providers showcasing cutting-edge payments & POS solutions.

Seniority breakdown



Geographical breakdown



mpe

WHO ATTENDED MPE 2019?

....just a small taste of companies attending MPE

Merchants

Desigual.
KLM
H&M
easyCoffee
bol.com
norwegian
Booking.com
TRAVIAN GAMES
CIRCLE K
amazon
Auchan RETAIL
Hello FRESH
STOKKE
IKEA
BOSS HUGO BOSS
NETFLIX
zalando
PORSCHE
Argos
Nestlé
adidas
BMW GROUP
Levi's
G2A.com

Industry experts

EY INNOVALUE
consult hyperion securing tomorrow's transactions
Edgar, Dunn & Company Management Consultants
Universidad Rey Juan Carlos
THE PAYPERS
pwc
JUNIPER RESEARCH
MERCATOR ADVISORY GROUP
EWPN MAKING DIVERSITY MATTER IN FINTECH
Aite

Vendors

ACI UNIVERSAL PAYMENTS.
Ravelin
Spire PAYMENTS Transaction. Interaction. Convergence.
IZICAP
HPS ENABLING INNOVATIVE PAYMENTS
ThreatMetrix A LexisNexis Risk Solutions Company
netcetera Software matters
RISK IDENT
Handpoint
Accertify InAuth
INFORM
NUAPAY
Merchant Suite
technologi
simility A PayPal Service
AEVI | DO MORE

Acquirers & PSPs

barclaycard
BNP PARIBAS
Worldline
adyen
Deutsche Bank
EVO PAYMENTS INTERNATIONAL
credorax
SBERBANK
INTESA SANPAOLO
mash
nets
Raiffeisen Bank International
UniCredit Bank
Elavon
VALITOR
PPRO the payment professionals
computop the payment people
BS PAYONE
Santander
ING
ingenico ePayments
BBVA
wirecard
Trustly

Schemes & regulators

mastercard
EUROPEAN CENTRAL BANK
UnionPay International
BRC
DISCOVER GLOBAL NETWORK
PCI Security Standards Council
AMERICAN EXPRESS
GS1 Germany
iDEAL
VISA

Full list is available to see HERE

MPE PHOTO GALLERY

Conference on 4 stages

Inspiring discusions

Networking & Workshops

2 exclusive dinners

MPE Awards

MPE 2019 in 3 minutes

To play, click below

Chair summaries from MPE 2019

David Birch
Director of Innovation
Consult Hyperion
(chair Day 1, Common program)

Once again the Merchant Payments Ecosystem Conference in Berlin turned out to be an absolute must-attend event for everyone in our industry. The range of topics, the organisation, the exhibition and the atmosphere were maintained despite the fact it is now grown to accommodate 1,000 delegates.

In my opening keynote, I said that I thought the nature of the changes facing the industry were now very different. This was hardly a random prediction, since it was founded on the comments made at last year's event around the new regulatory landscape that we see in front of us. Last year some of the features in that landscape, such as PSD2 and GDPR, seemed a little distant and hazy, but this year they are shaping and constraining the strategic routes available to us.

This led to a great emphasis on open banking, which I think was fully merited. I don't doubt that many organisations have had to change their view of open banking from being something technical to do with APIs and therefore the province of the technologists and scramble to respond to the new realisation that it means a fundamental reshaping of the industry and the creation of wholly new intermediaries, transactions and business models. Since these are what the conference is all about, it is no surprise that several sessions were dominated by discussion of stakeholder strategies and tactics in the context of the September 2019 deadline for the pan-European implementation.

If I had to pick out a couple of presentations that illustrated these changes very well, I would first direct attention to the presentation of IATA Pay by IATA (The International Air Travel Association) and Deutsche Bank. They are delivering a direct-to-account payment offering into the industry and I'm sure they will be only the first of many both horizontal and vertical sector-specific plays that will use the PSD2 APIs in combination with instant credit transfer to reshape the retail payments space in the medium term. I would also highlight the presentation of BankingBlocks who presented the potential obtained from rebuilding core banking infrastructure for this new API-centric environment rather than adding a thin veneer to legacy infrastructure and hoping for the best.

> "MPE is going from strength to strength. It's an essential conference for merchant acquirers, their customers and suppliers."
>
> Geoffrey Barraclough, EVO Payments International

Alan Moss
Director of Commercial Solutions in EMEA
InVue
(chair Day 1, Checkout & Conversion stream)

Session 3 - E & M Commerce trends driving innovation

- We had a strong focus on the issues of supporting multiple payment methods in many different geographies, online as well as face-to-face, with mobile providing a seamless bridge between the two worlds
- Seen from the Booking.Com perspective this resulted in building their own platform which they have been able to scale up and deploy internationally, to give their customers a consistent experience wherever they are
- From the perspective of Modo Payments, this gives an opportunity to be a facilitator for many different payment flavours, providing interoperability and taking the pain out of payments for retail and banking partners
- For Amazon Pay in India, the challenge is definitely one of scale, going from online to face-to-face, but with an enormous opportunity of 59 M micro-merchants to play for with their innovative QR-code solution
- Getting back to the online world, EMV 3D secure 2.0 continues to demand attention, with much interest focused around who is driving it, and whether issuers, PSPs and acquirers will be ready for the mandated European introduction schedule in October 2019.

Session 4 - Payments for digital merchant segments

- We had a great intro from Discover, showing how today's digital consumer really holds the key, and experience is what they value most critically, being seen in terms of Convenience, Context and Control. Quoting Justin Trudeau, "the pace of change has never been so fast, yet will never be this slow again"
- Building on this concept, Manja Pfeiffer took us into what the consumer really sees in online content, and how supporting micropayments will allow digital content providers to expand their revenue streams
- Anna Tsyupko from Paybase expanded further on this thread, really inspiring us to see payments as a key differentiator for online businesses, and outlining the criticality of holistic payment solutions for the marketplace model
- The same thoughts were echoed by Limonetik's Christophe Bourbie who described the complexity of marketplace requirements across multiple typologies, and the ability of well-designed payment systems to be a means of driving customer loyalty
- From the perspective of HelloFresh, a digital merchant with very tangible and time-sensitive product, supporting recurring payments is of the essence, and a key means of fostering a sticky customer relationship
- Although we discussed the importance of compatibility issues, be they PSD2 or 3D Secure 2.0, there was a real feeling among all participants that payments should not be treated as a potentially awkward and preferably invisible part of doing business, but as a means of improving consumer engagement, strengthening the customer relationship and increasing revenues.

Geoffrey Barraclough
Head of Proposition
EVO Payments International

(chair Day 1, NextGenPOS stream)

It's an exciting time at point of sale. Many of the innovations introduced in the past few years have gained widespread adoption; notably contactless and tablet-based software systems with their associated ecoystem of SME business applications.

At MPE, we heard from Juniper Research that contactless has reached tipping point in most major European markets. It is fast becoming ubiquitous for low value transactions. The technology is moving from retail to other sectors as was explained in an excellent presentation from the Milan Transit Authority which has introduced tap and go across its City.

Two restaurant specialist software vendors (ISVs) – Gastrofix and Touchbistro – showed how the easy integration of new and exciting apps via published APIs brings huge value to their customers. I was particularly taken with Table Duck, a chat-based order-at-table service that Gastrofix's customers can access.

The challenge for payment service providers is of maintaining brand differentiation and premium pricing when ISVs are orchestrating the small business ecosystem. One solution is for the acquirers to build their own application marketplaces delivered via SmartPOS devices. NEXI, the leading Italian merchant services provider, demonstrated what is probably the largest such implementation in Europe for which it has collaborated with Poynt.

Finally, there was much discussion on the latest POS payment technology - PIN on software also sometimes called PIN on common off the shelf devices (COTS). Californian start-up Magic Cube showed how this allows any Android device to become a payment terminal. The technology could be used either to produce ultra-low cost acceptance devices for micro-merchants or (more interestingly in my view) to create new and exciting point of sale technology for large retail.

Martin Koderisch
Manager
Edgar, Dunn & Company

(chair Day 2, Checkout & Conversion stream)

Five interrelated themes emerged from the fraud & security sessions. Secure Customer Authentication (SCA) , 3D Secure, data sharing / collaboration, biometrics and digital identity data, and finally Big Data Analytics, AI and ML. All five underpin the growing importance of data in fraud & security both in terms of the actual data being gathered but also how that data is communicated, shared and analysed.

1. Secure Customer Authentication: With just of 200 days to go before the Sept 14theffective day, interest in SCA was front and centre during the session. It is clear that there is a general lack of merchant awareness and to some extent misunderstanding of the SCA rules. Concerns were raised over the lack of card ecosystem readiness. Exactly what steps merchants should take to prepare for SCA were discussed in detail with various options considered. On the one hand, speakers emphasised the continuing need for merchants to score risk and outlined a strategy which would allow merchants to continue to make decisions about when to step-up to full 2 factor authentication. The message was clear. If Merchants wish to pursue this approach, they need to check whether their current acquirer can support TRA exemptions (in terms of meeting the fraud reference rates published in the EBA RTS) and if not, find one that can. Others challenged the futility of this approach given that, in the end, issuers have the legal responsibility to make a risk decision and have a 'final say' regardless whether an acquirer has applied the TRA exemption. An alternative SCA approach for merchants focuses on collecting and sharing data upstream to enable issuers to make a more informed risk decisions. A hybrid approach would see the merchants passing a risk score up to the issuer and flagging for low risk transactions and requesting an issuer apply a TRA exemption. In the end, which ever strategy is chosen, the new normal post SCA reality is that merchants will not be able to fully guarantee or control their customers check out experience. Regardless of how a TRA exemption is applied, merchants can greatly increase their chances of a frictionless flow by focusing on collecting and sharing data. Moreover, identifying who the key issuers of the cards most commonly used by their customers, and developing a solid understanding of those issuers SCA intentions, and potentially engaging with them to, at the very least, notify them of the steps they are taking to share data with the issuer community, is a sensible approach for merchants to take.
2. 3D Secure: The session also discussed 3D Secure as a compliant SCA solution for the card world, and highlighted that EMV 3DS or version 2 of the protocol is the go to solution that schemes are advocating and mandating their members to support. A liability shift comes into force in April whereby, any member that does not support 3DS2 will automatically have liability for that transaction. A central feature of 3DS2 is the ability for merchants to share far more data with issuers, and so connects nicely with the SCA conclusions above. However, given recent surveys suggesting many issuers are planning to migrate late, major concerns were raised about ecosystems readiness. The best case scenario is that the full ecosystem supports 3DS2 by Sept '19 and delivers all the benefits that the protocol has to offer including a far improved customer experience that will not result in the card abandonment rates previously experienced with 3DS version 1. However, a more realistic scenarios sees patchy support of 3DS2 and therefore a real risk that customers may experience completely different check out experiences with the same merchant depending on the issuer. It was felt that consumers may quickly work out which of their cards support the best experience, and hence incentivise issuers to move to 3DS2.
3. Data sharing / collaboration: Panel recognised that industry wide collaboration is becoming more essential now the ever to combat fraud. However, greater collaboration is being held back for a number of reasons. Banks reluctance to share transaction data with competitors, concerns over misuse of data shared in good faith, practical constraints of integration efforts, data prep and overall data compatibility. Nevertheless, progress towards connected datasets is evident with growing number of risk engine feeds commercially available.
4. Biometrics, Device finger printing and digital identity data: Panel discussed the future of biometric technology for authentication. In particular facial recognition technology with advanced 'liveness' tests which make blinking and eye movement tests more difficult to spoof. Mass of data available through device fingerprinting and mobile app and browser session data was also discussed. As well as other behavioural and other data sources such as key stroke analysis, wifi location, battery charge etc. All together this data - customer generated, device and from other data sources - provide enormous potential resource for risk detection. Identities can be analysed in real time and checked for anomalies compared to normal behavioural patterns. This type of passive authentication in which the user may not even be aware of the authentication check taking place in the background, raises ethical questions as well as data privacy concerns. For example, when does collecting of device and other behavioural data become sufficiently specific to become personal data and fall into scope of GDPR.
5. Big Data Analytics, AI and ML: Finally, the combination of the all the above - new regulatory security requirement to collect and share data, new 3DS2 pro-

tocol which emphasises data collection and sharing, growth in data collaboration, the mass of new digital identify data from biometrics, device finger printing and behavioural data - is accelerating the adoption and usage of big data analytics, AI and ML. The panel discussed latest AI/ML solution approaches that provide explanations into why decisions were made rather than black box AI models where decisions are made without any explanatory context. Link analysis and visualisation to show how decision attributes are related is also a key trend. AI/ML models also need decision orchestration i.e. ability to automatically decision customers and step-up when necessary, or flag high-risk applications and transactions for further manual review.

These five interrelated themes provide a clear direction of how the technology to fight against fraud is developing and how regulations such as SCA provide a more standardised framework for industry to work with. It will be interesting to the impact at next year's MPE by which time SCA will have taken effect.

Janusz Diemko
Member of
the Supervisory Board
Polskie ePłatności
(chair Day 2, NextGenPOS stream)

European POS Payments in 2019

Presentations in this session covered value added products at the POS earning airline miles linked to payment cards (Marco Aeschbacher – Worldline), experience of implementing tap and go at Milan subway and future expansion to other parts of the mobility ecosystem (Stefano Favale – Intesa Saopaolo / Roberto Andreoli – ATM), POS development and trends in CEE, interchange and country peculiarities (Andras Bakonyi – Raiffeisen Bank International) and possibilities for use case of Sepa Instant Payments based on reviewing the German market trends (Ercan Kilic – GS1); for the panel Anders Roe Edvarsen of CircleK joined. There is still too much complexity in the payments ecosystem and merger activity is not leading either to platform consolidation nor simplification of the omnichannel experience. Sepa instant payments has the potential other than to reduce merchant cost, but also to simplify the payment journey but it's early days yet to see how a unified customer experience will be achieved whilst reducing complexity for the merchant. The difference in EU / NON EU payment methods, interchange rules and regulations in general make supporting a merchant across various markets with a plethora of payments methods, in a unified manner a complex and difficult and sometimes an exasperating experience especially for the multi country merchant. For transport contactless payments though has made the operators and travellers lives, easier and much simpler and in conjunction with a payment app linked to other mobility methods (cars, bicycles, buses, trams) which will for allow a smarter city, lower travel costs and a more unified experience.

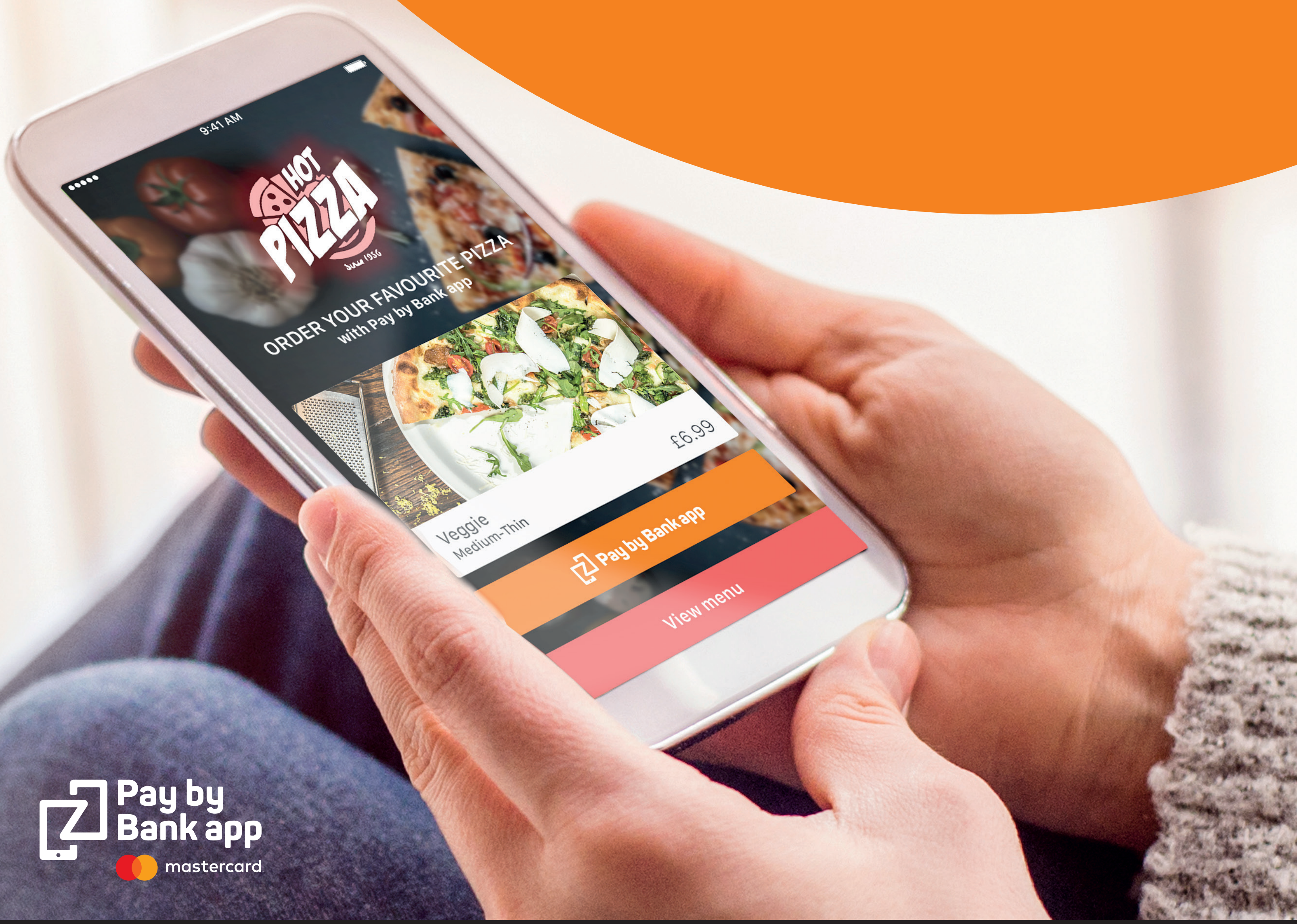
Pursuing the Omnichannel

Presentations covered an overview of integrated cross country payment infrastructure and the lack of a fully integrated infrastructure(Paul Prodrick - Elavon), how to support merchants omnichannel needs and channel hopping (Angus Burrell - Valitor) and incorporating omnichannel experiences in point of sales systems at

Making paying online easier

Designed to simplify the checkout experience. Pay by Bank app, allows consumers to pay online directly from their mobile banking app without the need to enter payment details or create new passwords or logins.

Using Request To Pay technology, the solution is regulation-ready, and apt for mainstream mobile payment adoption.



Pay by Bank app

mastercard

paybybankapp.mastercard.co.uk

large sports and other venues (Alexandre Armange - Digifoods). For the panel Boris Greisinger from Hugo Boss and Massimiliano Gallo joined. Omnichannel though is not for all merchants, so in planning the customer experience one needs to ensure coherence with the brand promise whilst avoiding consumer cul de sacs; dead ends adding no value to the customer. In the experience economy friction in the end to end process needs to be minimised and neither the hardware nor the software itself is the key but a seamless integration into a whole which provides the customer an amazing experience across all the various payment methods and touch points is; such as tapping any card to enter the metro, or ordering food via mobile app delivered at a football match to your seat, paying quickly at a fuel pump or enabling a consumer to browse, buy, and collect in the most convenient manner.

The key consideration from both sessions is that the customer is key and the customer experience journey is critical in ensuring customer satisfaction which translates to loyalty and increased sales. The payment process is just a part of this but needs to be as frictionless, convenient and simple as possible. The customer experience must also be tailored to both the brand promise and the customers needs and expectations. Over the next few years the continuing explosion of innovation around payments, omnichannel, checkouts point of sale devices will lead to improvements in the payment process for customers and merchants and its up to the industry to innovate and implement this for their benefit. This can only be achieved through cooperation with all the players in the industry, banks, acquirers, processors, PSP, software integrators and the device hardware manufactures.

David Parker
CEO
Polymath Consulting
(chair Day 2, Open Banking Ecosystem stream)

Open Banking collaborative ecosystem & Open banking and cross-border Sessions

Whilst it you could say a key theme of the whole conference was PSD2 open banking in the two sessions I chaired we delved down a bit deeper into the issues. The key outakes, and general agreement was:

- Some would argue that open banking has been around for a while already before the new September 14 deadline and was has launched so far has not had strong take up
- The RTS by not being more specific on the technical standards has resulted in a highly fragmented API market that could potentially inhibit growth
- It is though too late to put the clock back and in the EEA there will never now be a single technical API standard although we may see this in other markets globally
- A large number of 9,000 ASPSPs will not go live by March 14 for external testing
- We expected to see multiple use cases emerge for the data, with some believing it is the SME sector that will see the quickest take up
- For the incumbent traditional banks PSD2 offers opportunities as well as threats
- Retailer take up of PISPs, especially at the higher transaction basket end of the market is likely to see stronger desire to take in order to reduce costs
- iDEAL in the Netherlands is a good example of how strong a pay from bank solution can become
- A potential development of PSD2 open banking and the data could be that banks become verifiers of someones digital identity although major issues around where liability would sit for such a service need to be addressed

Ghela Boskovich

Head of Fintech & Regtech Partnerships

Rainmaking Innovation

(chair Day 2, Payment Ecosystem stream)

Panel 1 Write Up

Three themes took centre stage during the session on PSPs in 2019, each one already a familiar theme, each one still a nuanced challenge.

First point of discussion focused on a lack of - and therefore a need for - global standards for payment systems. Whether or not it is actually achievable remains to be seen, as market to market customer behavior is still culturally relevant, and alternative payment methods still vary market to market in degrees of adoption. Moreover, globally 93% of retailers do not have a unified payments experience for the end customer. Poor customer payment experiences cost merchants $10 billion annually, with a 55% purchase abandonment rate at the point of sale.

This fragmented payments experience is also complicated by tightening regulatory requirement for authentication, stronger security, and fraud oversight - a timely reminder that the 14th of September strong customer authentication deadline looms. The question of how to balance fraud prevention and security with experience expectations highlighted the staggering opportunity cost to both merchants and customers - nearly $21 billion annually.

The finale tune of the three themes was the opportunity cost of legacy systems, and a lack of true omni-channel seamless payment experience. The rise of e-wallets, mobile, and contactless payments either online or at the point of sale is taxing the archaic (or rather, less than modern even if only 5 years old) architected payments rails of most merchants. So how do we make it economical for the majority of merchants to manage the growing number of alternative payment types and oversaturated PSP market? One answer is to provide As-A-Service backends, focused on the value added services of onboarding, monitoring, and finance: to not own the infrastructure, but to leverage SaaS models that standardize the process, but allow for customized front end, on the glass experiences. It's about access to standardized systems, with a personal customer-centric touch.

Panel 2 Write Up

What do PSPs need to do to adapt to a dynamic market and ever evolving regulatory landscape? A few answers bubbled up during the debate on stage.

First off, PSPs as lenders and a source of credit was a bit part of the conversation. New business models advocate for going beyond the traditional PSP remit to include access to credit, specifically SME lending based on card payment revenues. Will this be a viable substitute for SMEs, giving them options beyond traditional invoice and asset financing? It looks likely, especially as the move towards instant settlement becomes a reality, and the opportunity costs to both PSPs and SME merchants of slower settlements also makes access to capital an interesting new offering.

Real-time reconciliation is also crucial for a PSP to stay relevant. With the complexities of multi-currency and cross boarder payments, and the vast volume of individual corporate accounts some merchants have on their books, accurate and instant reconciliation becomes the name of the game.

A Mobile-first approach is also de rigueur for PSP relevancy. Despite individual markets remaining culturally sensitive to preferred payment types, the industry still has to satisfy the consumer demand for mobile payments. Enter stage right the Chinese model, and its whopping 75% mobile payment adoption rate. The model may not work for Europe, but it shows that legacy systems will be outpaced (and their cost of ownership/use will be high not only in operational expense, but in opportunity costs as well) - and small merchants entering the market, especially e-commerce merchants, will opt for the cost savings of a purely digital/mobile PSP experience.

And underpinning this entire discussion is the question of security standards vs customer convenience: how to strike the balance between the 3-domain security authentication standards anti-fraud mechanism and the ease of the customer experience. Since experience has shown that highest levels of security and fraud prevention actually lead to significant purchase abandonment rates, striking the balance matters. Will tokenization solve this problem, and serve as the next sort of "global standard" for card and alternative payment methods? We should have a clearer perspective on that at MPE 2020, so check back with us next year.

Paul Rodgers
Chairman
Vendorcom
(chair Day 3, Checkout & Conversion stream & Conference outcomes discussion)

In opening the payments compliance challenges session, we had a distinctly automotive theme from Ian Butler at Elavon who drew parallels to the evolution safety systems throughout the development of the motorcar. What might have been acceptable in the past in automotive safety is no longer tolerated and that industry has made a robust response to securing the public. We are probably at the automotive equivalent of the 1970s in the payment ecosystem when it comes to securing consumers and the challenge for the industry is to take a similar response to embedding secure systems – the equivalent of the ubiquitous airbag - across the payment Infrastructure.

The presentation from Martin Koderisch at Edgar Dunn tackled the Regulatory Technical Standards for Strong Customer Authentication head-on. The payments sector challenge is to collaborate to fast track solutions for this demaning regulation where the enforcement deadline is less than 200 days away!

Andrew Cregan from the British Retail Consortium was on typically robust form, highlighting statistic after statistic showing the ever-increasing costs of accepting card payments despite the interchange fee regulations having been applied over three years ago. Clearly the European regulatory environment has not had the desired affect and merchants remain challenged by this cost of doing business.

The fact that the GDPR compliance deadline was almost nine months ago doesn't mean that everything is done and dusted! In a useful reminder of the ongoing challenges that merchants payment except organisations have in complying with GDP are, Derek Fattal from BlueSnap give an insightful presentation.

With the four presentations concluded, the presenters were joined in a panel discussion by Andrew Mitchell from JCB International

Much of the panel debate on payments compliance challenges centred on the regulatory technical standards for strong customer authentication.

This discussion then broadened to look at the role that regulators have in driving innovation in the sector. Whilst it was accepted that a regulatory mandate can catalyse the market to the payment change more quickly than market forces would permit, it was also recognised that regulators have a relatively poor appreciation of the nuances of merchant market dynamics and risk creating an uncompetitive economy for all. Certainly, the on realistic timeframes for the adoption of regulation polls huge structural and financial challenges to the merchant market and risk confusing the citizen-consumer end user.

In the fraud and security session we were concentrating on card not present fraud protection. Our opening presentation from the Head of Cybersecurity at MasterCard was a lesson to everyone in terms of the scale of the battle that we are facing! The fact that fraudsters have few barriers, instantly puts the legitimate financial services sector fraud protection bodies at a disadvantage.

One of the clearest areas where the card schemes have come together in a collaborative response to the threat through the work of the PCI Security Standards Council. Jeremy King, their International Director, gave a comprehensive update on all the activities that this group is delivering solutions providers and merchants.

One of the greatest examples of a collaborative approach in fraud protection is the work of Ethoca and their EVP of Business Development, Trevor Clarke give some clear examples of how to bring data from solutions providers and merchants together to help tackle card fraud.

David Newman, from the automated decisioning software solutions provider Forter (which had won the Best Anti-fraud Solution award at the previous evenings MPE awards), joined the previous presenters in an engaging debate and discussion.

This panel focused on how we can turn the tables on the fraudster and the overarching theme for the discussion was how is the payment sector collaborate more effectively.

The closing plenary panel discussion saw some of Europe's leading activists in the payments landscape coming together to, quite literally, debate some of the most pressing topics that are facing the industry. I was privileged to chair the session and, whilst it was always going to be impossible to cover to the wide range of topics that are challenging the industry, we managed to look at the ongoing debate about the role of cash in payments acceptance, what Open Banking and PSD2 offers to businesses and consumers, and the regulatory threat to the economy of the Regulatory Technical Standards for Strong Customer Authentication.

In wrapping up the session I challenged each of the panellists to put themselves in place of the audience and suggest what the key things to focus on would be when they were back in their businesses in the coming weeks and months. At last we have some agreement between the panellists! The overwhelming response was that delegates should make sure that they are as informed as possible and start putting their businesses on the path that will allow them to adopt the best of the innovations and developments that are sitting on the horizon in this fascinating payments landscape that we all occupy.

"Excellent event to exchange and network with peers in payment space. Perfect mix of size, setting and relevant attendees for good conversations."
Mrdjan Uzelac, AEVI - DO MORE

"One of the best networking opportunities in the Payments Industry."
Alana Kazykhan, paysafecard.com

PowerCARD

Gary Munro
Principal Consultant
Consult Hyperion
(chair Day 3, NextGenPOS stream)

NextGenPOS: Day 3 Session 1 – Retail reimagined

Retail reimagined looked at how technology is changing the in store shopping and payment experience. Changes in how we pay, what we pay with and how we authenticate are all moving apace. In turn this is bringing more ways to connect the shopper to the goods they wish to purchase and how they wish to pay for them. The challenge here is to ensure that payments are both frictionless and secure, two things which don't always go hand in hand. An excellent group of speakers and panellists helped us understand this change and how it will bring about improved retail experiences for us all.

Ward Hagenaar from Connective Payments set the scene by showing how leading brands are deploying the technology to create better personalised experiences, localised trends and targeted solutions. Order ahead and try in the fitting room takes click and collect to the next level.

Sami Karhunen from OP then explored the payments aspect, and how biometrics are revolutionising how people pay. The example of setting up a PoC facial biometric payments systems from scratch in just 3 months shows how new technology and APIs are simplifying the integration process and shortening the timescale to bring new technology to the retailer.

Francois Lecomte-Vagniez from the Smart Payment Association then discussed the importance of securing these services, in particular the payment aspects, particularly as the payment instruments become embedded into the connected world, such as the car. As we move from pull to push payments the security of access to the funding account and the ability to provide a trusted payment experience become paramount.

This lead neatly into the presentation by Nick Telford-Reed from Stormglass Consulting explored how web payment standards were advancing and the affect these would have on the retailer. The work of the W3C, EMV with Secure Remote Commerce and the FIDO alliance are all seeking to simplify the payment experience from a browser of mobile device. These changes, plus the development of PCI standards such as SPoC are not good news for the traditional POS device. The future of payment acceptance is in software not hardware. A theme which nicely set up the following session.

NextGenPOS: Day 3 Session 2 – New Revenue Streams for POS

Building on the 1st session, this session explored how we need to change our understanding of POS.

Diderik Schonheyder explained how the standalone secure boxes we know, with long development and upgrade cycles are no longer fit for the modern retail space.

Petr Menclik of Dotypos described how the retailer needs a flexible, software based POS environment in order to be able to provide the services and payment methods most appropriate to the shopper. Something which the POS behemoths of today are struggling to understand. Moving to a Software as a Service model enables fast update cycles and simpler feature integration, and also enables the microbusiness to gain access to data and consumer insights that were previously out of reach.

Ergi Sener of IdeaField then layered the sensor and AI technology which would enable the retailer to maximise the experience the customer's visit and provide simple additional services to ease and improve their experience.

This led to a fascinating panel discussion on the ethics of retailers tracking the movements of staff, customers and payments in order to provide the optimal experience. It was pointed out that this is no different to what someone experiences when they shop online, but the transfer of privacy for a better retail experience in the real world is not without its challenges.

Benjamin Kirschbaum
German attorney at law
WINHELLER law firm
(chair Day 3, Payment Ecosystem stream, Session 1)

On the blockchain session it has been demonstrated that the adoption of cryptocurrencies as a means of payment is still very limited in most parts of the world. Reasons given were the high volatility of cryptocurrencies which make it very difficult for businesses to calculate with cryptocurrencies. Also the increasing valuation makes cryptocurrencies more of a speculation object than a means of payment. Scalability issues were also mentioned. In addition to these problems there were also concerns of consumer protections raised. When you pay via credit card or Paypal you have it very easy to charge your money back, while if you pay with cryptocurrencies no such chargeback is possible. While this is bad for the consumer it could be advantageous to businesses since they do not have to deal with fraudulent chargebacks. This is especially apparent in industries like gambling.

One of the most important areas where cryptocurrencies can be advantageous has been identified as cross border payments. While Ripple Labs are focussing on making the bank-to-bank market more efficient, the cryptocurrency Dash targets the consumer to consumer market. Both parties have innovative concepts to allow instant cross border payments. In the case of Ripple this even functions as a currency exchange, so you can send US Dollar and receive Mexican Pesos. Besides the development of the technology this process needs a lot of partners like banks, cryptocurrency exchanges and so on.

Lastly the participants agreed that the Blockchain is a great idea, but that there are a lot of illogical, unnecessary or outright fraudulent ideas out there, that basically use the word "Blockchain" as a marketing ploy. The ICO market in 2017 was especially prone for fraud. But the blockchain as a method of the storage and transfer of value had universal appeal and will be a relevant force in the future. Regulation of the cryptocurrency and blockchain space is welcomed to facilitate further adoption. But the relevant stakeholders have to make sure, that it will be good regulation and not bad regulation.

> "My first year with MPE -the one in 2019. Didn't regret even a second that decised to participate. Definitely will come next year."
>
> Ewa Stanska, Boomer Sky

Rogier Rouppe van der Voort
CCO
Payments & Cards Network
(chair Day 3, Payment Ecosystem stream, Session 2)

Participants in the panel discussion on B2B payments were Christophe Bourbier of Limonetik, Max Bense of CollectAI, Frauke Mispagel of Otto Group Digital Solutions and Daria Rippingdale of Banking Blocks, which was hosted by Rogier Rouppe van der Voort of Payments & Cards Network. The panel gave us a taste of what B2B payments look like and what the impact of regulation and current market developments is.

Key takeaways of the session are that current underinvestment and falling behind of traditional banks have caused new players in the B2B space to offer better, faster and cheaper services. Whilst traditional banks are busy adhere to new regulations such as PSD2 and GDPR, FinTechs see regulation such as PSD2 as an advantage as real time payments offer shorter remittance cycles and are therewith less risky which makes digitalization for B2B corporates much easier.

B2B corporates require a lot of education when it comes to B2B Payments and development is lagging behind compared to B2C payments. The old-school invoice is replaced by only payment methods and B2B payment providers offer the full payment cycle, from collection to settlement to reconciliation, or even complete core banking platforms that corporates can modularly plug into.

“MPE is a must attend event for payments professionals as the subjects chosen for discussions & presentations are very topical and you get to hear from some of the sharpest minds in business. Opportunities to network are nicely weaved in to the agenda ensuring you get maximum value from your participation.”
Amit Kurseja, Amazon Pay India

TOP rated speakers
based on feedback from MPE participants

David Birch
Director of Innovation
Consult Hyperion
with speech about Blockchains and Blockheads

Martin Sweeney
CEO
Ravelin
with speech about "Acceptance Maximisation"

Bartosz Skwarczek
CEO and Founder
G2A.com
with speech about "A Short Journey Into Dangerous Territory"

Andras Bakonyi
Group Product Manager Card Acquiring
Raiffeisen Bank International
with speech about "POS Payment Development in CEE"

Go Mobile | Go Global

Handpoint*

Enabling merchant acquirers to take charge of the mPOS and NextGenPOS game

Day 1 - 13:50 Presentation
From MobilePOS, to NextGenPOS, to NoPOS.

Come meet Handpoint at Stand P01

www.handpoint.com

mpe Merchant Payments Ecosystem

19-21 February 2019, Berlin

SPONSORED BY: DISCOVER GLOBAL NETWORK

MEDIA PARTNER: THE PAYPERS

MPE AWARDS 2019

„THE EUROPEAN MERCHANT PAYMENTS AWARDS“

MPE Awards 2019

The only European Awards recognizing top European merchant payments acceptance companies and their achievements

MPE Awards 2019 recognized TOP 12 European merchant payments providers at 12th annual MPE 2019 (Merchant Payments Ecosystem) conference and exhibition during the Gala Dinner in front of 1000+ senior industry professionals.

For night years in a row, the MPE AWARDS serves as a quality benchmark in European merchant payments and helps merchants in decision making over the payment pro- viders. For 2019, the categories have been fully updated to reflect the areas that matter most to payment acceptance in today’s market.

The MPE 2019 Awards Gala Dinner & Ceremony, took place on February 20, in the prestigious Five Star Intercontinental Hotel Berlin. Awards Gala Dinner was hosted by recognized payment industry advisors & speakers: Alex Rolfe & Ghela Boskovich.

PEOPLE'S CHOICE AWARD winner

MPE Influencer of the Year Award: **Newgen Payments**

JUDGE'S CHOICE AWARDS winners

Best Acquirer / Processor of the Year Award: **PPRO**

Best PSP Award: **Yandex.Money**

Best On-Boarding Process/Solution Award: **Technologi Worldwide**

Best ID, SECURITY & ANTI-FRAUD Solution Award: **Forter**

Best POS Innovation/POS software Payment Applications Award: **myPOS Europe**

Best Alternative Payment Solution Award: **Banking Circle**

Best International/Cross Border Payment Solution Award: **ACI Worldwide**

Best Merchant Payments Partnership Award: **Handpoint**

Best Data Analytics & Science Award: **Nets Group**

Best Merchant Payment Implementation/Process Award: **Computop**

Best Start-Up Innovation Award: **MuchBetter**

newgen INGENUITY REDEFINED

WINNER IN CATEGORY

MPE INFLUENCER OF THE YEAR

MPE AWARDS 2019

"MPE Influencer of the Year" Award went to the most influential payment provider for the significant contribution to the growth and development of the merchant payments industry during the last year.

Click here to watch the interview

PPRO
the payment professionals

WINNER IN CATEGORY
BEST ACQUIRER / PROCESSOR OF THE YEAR

MPE AWARDS 2019

This Award went to the outstanding Acquirer who has developed an excellent acquiring service for merchants throughout Europe.

TRISTAN CHIAPPINI
Head of Account Management, Payment Services
PPRO Group

Click here
to watch the
interview

Yandex money

WINNER IN CATEGORY

BEST PSP AWARD

MPE AWARDS 2019

This Award went to the PSP who offers the best and most efficient mix of payment options and/or providing the best overall service to its customers and/or supports merchants' omni-channel payments strategy – the availability of all payment options in any channel.

Click here to watch the interview

technologi

WINNER IN CATEGORY

BEST ON-BOARDING PROCESS/SOLUTION AWARD

MPE AWARDS 2019

Went to payment providers for customer-focused on-boarding process/ solution meeting merchant demand for fast & convenient on-boarding.

Click here to watch the interview

FORTER

WINNER IN CATEGORY

BEST ID, SECURITY & ANTI-FRAUD SOLUTION AWARD

MPE AWARDS 2019

Went to the provider, who has the best performing security system, Best Identity Verification and Authentication Solution as expressed by merchant satisfaction, fraud & chargeback rates or security breaches.

Click here to watch the interview

WINNER IN CATEGORY
BEST POS INNOVATION AWARD

Went to provider for best use of integrated POS / Smart POS / Mobile POS solutions to merchants and/or SMB helping them to accept payments, improve business results with value added services and revolutionise the customer shopping experience in-store.

Click here to watch the interview

BANKING CIRCLE

WINNER IN CATEGORY

BEST ALTERNATIVE PAYMENT SOLUTION AWARD

MPE AWARDS 2019

Provider or solution that most effectively facilitates merchant payment payment transactions without requiring the consumer to directly use a payment card, i.e. methods like OBeP, open and closed wallets, cryptocurrency payments, in-app payments, direct-carrier billing, etc.

MISHAL RUPAREL

Senior Director, GM Europe
Banking Circle

Click here
to watch the
interview

ACI UNIVERSAL PAYMENTS℠

WINNER IN CATEGORY
BEST INTERNATIONAL
PAYMENT SOLUTION AWARD

MPE AWARDS 2019

Went to the provider who did set-up the best offer, programme, or system, to service international merchants.

RICHARD JOLLY
Director, Business Development eCommerce, Fraud&Omni-channel
ACI Worldwide

Click here
to watch the
interview

Handpoint

WINNER IN CATEGORY

BEST MERCHANT PAYMENTS PARTNERSHIP AWARD

MPE AWARDS 2019

Best enhancement or design/ development of payment product/ solution/service prepared through acquisition, collaboration and, or partnerships by and between payment technology providers, payment companies, merchants and POS solution providers.

Click here to watch the interview

nets

WINNER IN CATEGORY

BEST DATA ANALYTICS & SCIENCE AWARD

MPE AWARDS 2019

Went to the provider for Best Data Management and Infrastructure; Best Use of Data in a Merchant payment Product or Service delivery and Best advanced analytics & Data Science.

mpe Merchant Payments Ecosystem
MPE AWARDS 2019
ANNA-KARIN OSTLIE
SVP, Head of Payment Services Norway
Nets Group
0:14 / 0:58

Click here to watch the interview

computop
the payment people

WINNER IN CATEGORY
BEST MERCHANT PAYMENT
IMPLEMENTATION AWARD

MPE
AWARDS
2019

Went to the Merchant for best payment process/implementation supporting seamless digital customer experience, online, in-store or mobile.

Click here to watch the interview

MuchBetter

WINNER IN CATEGORY

BEST START-UP INNOVATION AWARD

MPE AWARDS 2019

This Award went to the winner of the Innovation Corner competition for the most innovative start-up company in Merchant PaymentsEcosystem.

Click here to watch the interview

Your merchants want more than just payments

MPE 2019 speakers turned their presentations into articles.
What they were speaking about? …

Brendan Jones
Chief Commercial Officer
Konsentus

The Challenge of TPP Identity & **Regulatory Checking for FIs** delivering PSD2 open banking

In January 2018 the European Union Payment Services Directive 2 (PSD2) came into force across Europe, delivering a consistent vision for open banking across all member states. Payment Service Users (PSUs), e.g. consumers and SMEs, will have a legal right to share their personal transactional account data from their Financial Institutions (FIs) with regulated third parties to enable better financial outcomes.

FIs must provide regulated third parties access to end user transactional account data. Key critical dates that FIs must work to, as directed by the European Banking Authority (EBA) and local National Competent Authorities are:

- March 2019 - FI's must have platforms available for external market testing
- Sept. 2019 - FIs must go live or face the risk of fines from regulators

FIs must comply with this regulation and can only provide data to regulated/authorised Third Party Providers (TPPs).

Who is Covered by PSD2 open banking

PSD2 uses the term 'Transactional Account'. The UK FCA defines a transactional account in the FCA handbook as a 'Payment Account' and a "Payment account" is defined in the FCA regulation 2 as:

"an account held in the name of one or more payment service users which is used for the execution of payment transactions"

So who is covered, almost every account that is accessible vis an online interface (i.e. mobile / internet banking etc.):

- E-wallet Wallet
- Reloadable Prepaid Card
- Bank Current and Payments Accounts

In total there are some 9,000 plus FIs in Europe that need to be ready for open market testing under mandatory PSD2 timescales.

The EBA recently stated: "Ignorance of them can of course not be used to justify non-compliance. And added, non-compliance amounts to a breach of law, with the resultant consequences for the legal entity."

The Challenge on Checking Who You Provide Data To

The regulations are clear that it is the job of the FI to validate the identity of the TPP and check their regulatory status, this is crucial to establishing the trust factor as part of the PSD2 open banking. This means that all FIs need to ensure that they only ever supply PSU data to approved/regulated TPPs. If they supply data to a TPP who is not, then they are in breach of PSD2 and GDPR.

When an FI is approached to provide data for the first time by a TPP they need to:

1. Validated the TPP eIDAS Certificate via the Qualified Trust Service Provider (QTSP) to confirm identity of TPP and associated National Competent Authority (NCA)
2. Check with the correct NCA that the TPP is regulated/approved
3. Issue the Access Token to the TPP as appropriate (PSD2 schema)

Then each time the TPP accesses the FIs API the FI needs to:

1. Validated the TPP eIDAS Certificate via the correct QTSP to confirm identity of TPP and associated NCA
2. Check with the correct NCA that the TPP is regulated/approved
3. Validate the Access Token checking that end user has not revoked Consent

Can FIs rely on eIDAS certificates?

Although Qualified Certificates and Seals provide some of the security mechanisms required by the PSD2 they do not provide all. The security and assurance that ASPSPs need to authorise a PSD2 transaction with a TPP across its dedicated interface, they need to know, in real-time, that:

- A TPP is still regulated by its National Competent Authority
- It is still approved to perform the role which is consistent with its API request
- The consents it received from the PSU are still valid, and have not been revoked by the PSU

However, verification of the TPP eIDAS certificate is not sufficient in itself. Qualified Trust Service Providers (QTSPs) have a legal obligation to validate the regulated status of a TPP, with the host NCA, at time of issuance of the eIDAS certificate(s). However, there is no requirement for them to subsequently check the status of TPP. The NCA also has no legal duty or obligation to inform a QTSP if TPP revocation has taken place and a NCA will probably not know who the QSTP is. The TPP eIDAS certificate thus states what regulated status a TPP held at time of issue, but not in the intervening period.

Is the EBA Register the solution?

Final Report on Draft RTS setting technical requirements on development, operation and maintenance of the electronic central register and on access to the information contained therein, under Article 15(4) of Directive (EU) 2015/2366 (PSD2), and Draft Implementing Technical Standards on the details and structure of the information entered by competent authorities in their public registers and notified to the EBA under Article 15(5) of Directive (EU) 2015/2366 (PSD2).

During the development of the CP, the EBA considered but disregarded the possibility of introducing a functionality in the EBA Register which would allow external applications to communicate automatically with the EBA Register. The EBA considered this 'machine-readable' functionality to be too costly for the EBA to develop and implement.

The EBA re-assessed the case for and against the development of an API and decided it would result in a significant increase in the implementation and operational costs for the EBA and could also delay the development of the EBA Register. The requested functionality was thus found to not be directly linked to the objectives of PSD2 related to the EBA Register in accordance with recital 42 of PSD2: increasing transparency, ensuring a high level of consumer protection and facilitating cooperation between the home and host competent authorities.

The result is the EBA database is not an online real time machine readable database. It is only updated twice daily with NCAs updating it once daily.

Are NCA Registers the solution?

There are 31 National Competent Authorities in the EEA and each NCA publishes data in a different structure, with different fields, many in different languages. Further each NCA publishes updates at different times, many in different ways. NCA Databases are also not generally machine readable, real-time. Some National Competent Authorities do not publish/state where TPPs have passported to and National Competent Authorities that publish "Inward Passporting EEA Authorised Firms" do not indicate which Home Member Sate passported from.
In Summary the Challenges of TPP Identity and Regulatory Checking

- The EBA Register is not an onlilne machine read-

able database
- National Competent Authority Databases are generally not Machine Readable
- National Competent Authorities have no legal obligation to notify Scheme Regulatory Databases other than a general published bulletin when they revoke a TPP
- National Competent Authorities have a 20 day SLA in place to notify passported NCAs when a TPP is revoked
- There are 70+ Qualified Trust Service Providers who issue eIDAS seal Certificates that need to be integrated to check on eIDAS certificates

Brian Hanrahan
Chief Commercial Officer
Nuapay

Open Banking – **Changing The way We Pay**

The Problem

In the retail world, either online or bricks and mortar, many customers opt to pay using cards, however the procedures involved in processing card payments are inherantly insecure. Merchants have to collect and store sensative information, the card details, so they can request the money from the card issuer at some future point in time. This stored data can be reused to make payments without the card owner's knowledge making it valuable to criminals and enabling fraud. To overcome this inherant weekness card schemes keep adding more and more complexity to the processes used such as PCI DSS, 3DS, CVV and tokenisation. Even so fraud rates continue to climb so what next? Added to this merchants identify cards as the most expensive way in which they can take a payment.

So is there a better way, can a system be designed that is more secure by design and offers low transaction fees?

Below we look at payment mechanisms built around the use of the recently introduced Open Banking functionality which has the potential do deliver these objectives.

What is Open Banking

The concept of Open Banking has been introduced by regulators partially to stimulate innovation and partially to introduce further competition into the finacial services market. Already introduced in the UK, the processes becomes mandatory within the EU later in 2019 and is formalised in the latest Payments Services Directive.

Open Banking allows third parties to either initiate a payment from a bank or to access account details of a customer at a bank. Clearly these activities cannot be performed by anybody at will so the third party provider has to be licenced and the individual who is a customer of the bank has to give their permission.

An Open Banking Option

Collecting a payment using Open Banking seems like a simple process. The first step is for the merchant to ask the customer which bank they want to use. An API call is then made to the chosen bank giving details of who the payment is for, the amount of the payment and details of an account into which the payment is to be pushed. In an online world the customer is then transferred to their bank's online environment where they log in using the bank's security, view the payment details and if they are happy confirm to the bank that they can make the payment. And that's it. The bank sends a status messgae via the API to the merchant saying the payment has been initiated and, in the UK, sends the money via Faster Payments to the specified account.

In this process there is no sensitive data about the customer presented to the merchant. All the merchant knows is which bank the customer uses. Not having to collect or store sensitive data about the customer means the merchant has nothing worth stealing, nothing that can be reused for another payment so no opportunity for fraud. Gone are the needs for hightened security, encryption or other compliclexities. Further the payment was made using Faster Payments which is charged at a low flat rate irrespective of the transaciton's value.

The Players

The process of executing the Open Banking payment is actioned by a suitably licenced organisation known as a Payment Initiation Service Provider (PISP). Whilst the process sounds straightforward the PISP has to be able to route the request to the customer's chosen bank, understand the structure of the bank's interface and also carry out security checks to make sure the request reaches the correct bank. With the UK implementation these elements are well defined within a centralised infrastructure but this is not the case in Europe where banks can individually define their own standards.

Process gaps

With the basic Open Banking process we thus have a process that it inherently secure and as an aside can get cleared funds to the merchant in a matter of seconds. The security aspects themselves though give rise to their own problems. For example take the case where the merchants needs to make a refund to their customer for whatever reason. By design the merchant does not know the account details of their customer and thus has no way to initiate a refund.

Implementing Open Banking can also become an issue for the merchant. Now all payments received will appear in statement data available from a bank. This data will be available electronically but the connection is unlikely to be one the merchant is familiar with, at least in this context. Further the format of the data will be unfamiliar to the merchant.

Unlike with other payment channels a merchant is likely to offer the payments will be received as individual items in the merchant's bank account. For the privilege of receiving these payments the merchant's bank will levy a charge for each transaction received. For smaller merchants these charges can be quite high confounding one of the target ambitions of using Open Banking.

Nuapay Approach

Nuapay, Part of the Sentenial group of companies is a licenced Payment Institution and provides payment and associated services to business of all sizes as well as supporting major banks, PSPs and merchant acquirers. Its platforms process over €42 billion each year.

Nuapay has implemented a cloud based service that delivers the benefits of Open Banking based payments and at the same time resolving the short falling exhibited by the base scheme.

From a PISP perspective Nuapay is licenced to deliver all Open Banking functionality within the EEA and as a part of this takes responsibility for establishing the routing and procedures required to give the merchant reachability to paying banks in this region.

To cover the gaps in the functionality provided by the base implementation, Nuapay exploits its capabilities as a Payment Institution by routing the payments into an account it manages. Having access to data from the interbank payment clearing system allows Nuapay to provide simple to use refund procedures, alerts for failed payments and an auto reconciliation process. Merchant funds received this way can be transferred to any external account at frequencies that suit the merchant.

As Nuapay processes high volumes of transactions it can offer very competitive rates for processing the payment. This aspect not only benefits the merchant but also lets Nuapay quote a total end-to-end price for the service. This contrasts to the position where the money is paid directly to the merchant's account as here the service provider has no control over this element of the merchants costs.

In common with all Nuapay offerings the service can be delivered by Nuapay itself or can be white labelled by PSPs or acquirers where the service can be provided in a way that mirrors those used for other payment channels delivered to merchants.

The Future

At present Nuapay is live in the UK market. This is possible as the UK Government mandated the introduction of Open Banking sometime ahead of the rest of Europe.

All banks in the EEA will have to provide the necessary interfacing capabilities by September 2019. As these banks become live Nuapay will extend its reach matching the availability.

Looking further afield the concept of Open Banking is becoming a global trend. Most developed economies either have or are planning Open Banking procedures, it thus thought that the benefits of paying this way will develop into a global norm.

For further information visit www.nuapay.com

Derek Fattal
Senior Legal Counsel
BlueSnap

GDPR – **Controller & Processor Compliance Issues** for Parties in the Transaction Chain

There are important legal issues that payment industry players need to take into account with respect to the ‘transaction chain,’ regarding the GDPR.

Payment businesses and their clients are faced with a high degree of uncertainty. The manner in which value and wealth is exchanged is shifting almost daily. Payments are being digitized and cash is set to be superseded by a host of new payment methods. Payments have become globalized and the market has even been subjected to political struggles between the world’s main economic powerhouses. Our personal identities and savings are ripe for attack from criminals. Change and disruption are part of the new order in addition to acting as catalysts for new opportunities.

Against this backdrop the GDPR aims to bring about some order and certainty with respect to the safeguarding and treatment of personal data. Minimum levels of corporate responsibility have been set out in the legislation concerning how personal data should be treated. Data usage and transfers have to be mapped and information must be handled and deleted responsibly.

The GDPR extends jurisdiction so that it applies to companies outside the European Economic Area that deal with data relating to individuals based in the EU.

In the spirit of prior legislation, the GDPR divides treatment of data between parties that are defined as ‘Data

Controllers' and 'Data Processors'.

The GDPR sets out four main 'roles' in the processing of data. 'Data Controllers' are the parties that normally determine the purposes and means of processing personal data –
this is often termed the 'Why and How' of processing. Data Processors meanwhile are parties which process data under the request of a Data Controller. This really touches 'What' processing is taking place.

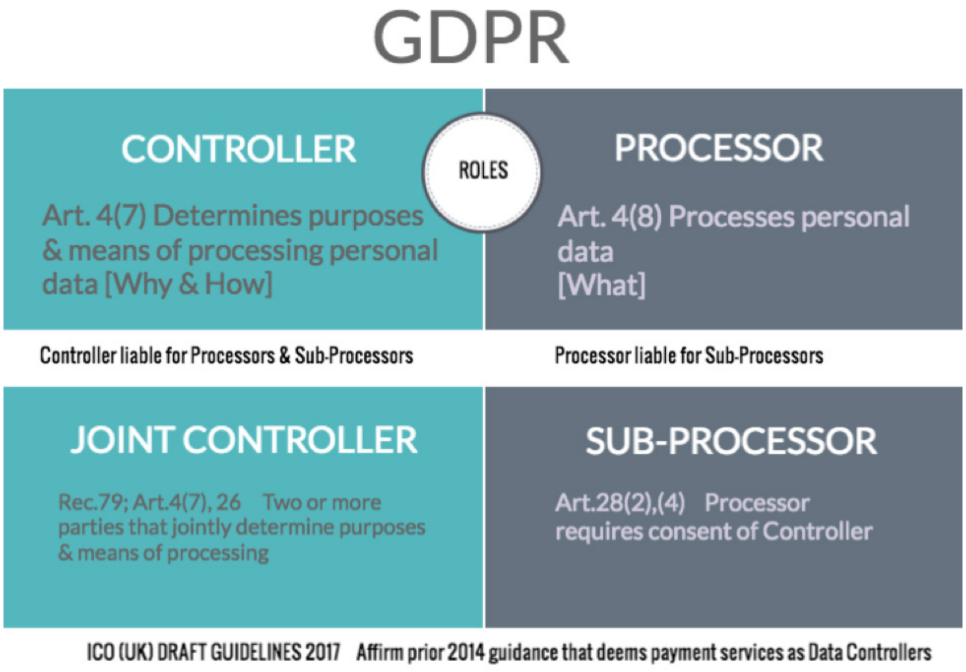
Data Processors can then, in turn, pass certain responsibilities onto 'Sub Processors' provided this is with the consent of the respective Data Controller. In addition, in certain circumstances distinct Data Controllers can be deemed 'Joint Controllers'.

Unfortunately, there is little up-to-date guidance as to how these roles are to be split between the different parties in the payment industry. The UK's Information Commissioners Office issued draft guidelines in 2017 that merely parroted previous guidance published back in 2014, stating that payment services would generally be deemed Data Controllers. Throughout there has been a failure to take account of the complexities involved in the multi-layered payments process. Data flows can be messy, a true nightmare to accurately map as transactions typically involve long payment chains with many intermediaries. As a result, the four broad legal processing roles do not readily fit the reality of transaction processes. Personal data usually moves from a Card holder to a merchant and then onwards. Shopping cart technologies will often be involved, not to mention subscription management services anti-fraud technologies, payment wallets, payment gateways, regional processors as well as marketplace models.

Determining and applying the Data Controller and Data Processor roles onto such complicated and often bi-directional movements of data can be extremely difficult in practice. Notwithstanding such uncertainty, the designations have significant impact concerning legal liability.

BlueSnap has devised a seven-point checklist of the key liability provisions that payment companies and merchants should take into account under the GDPR. Let's examine these in turn.

1. The threats of the big fines that regulators can impose under the GDPR were met by a loud fanfare that helped galvanize many businesses into action. These must be taken seriously, with the maximum amount being the higher of 4% of global turnover or €20 million.
2. The greatest liability impact does not come from the regulators but rather the liability that stems from the Data Controller and Data Processor relationships. Under the GDPR, liability generally flows down the data processing chain. This means Controllers and Processors are each directly liable for breaches by parties connected down the chain.
3. Under Art 82(4) each of the parties involved in the same processing may be held liable for the entire damage to a data subject. The data subject needs to be paid out in full before parties can begin to recoup from the true culprits in the chain.
4. Art. 82(6) gives claimants a choice of jurisdiction that opens the way to forum shopping, choice of targets and the selection of legal systems that are more supportive of class actions.
5. Data Subjects have rights to claim for an infringement of any rights afforded under the GDPR. They can bring those complaints to the regulator and even mandate a privacy rights organization to pursue those rights on their behalf.
6. Data claims can cover special damages and non-material damage further inflating liability to include financial loss and distress.
7. Joint Controllers may be jointly liable for the acts of their fellow joint controllers. This could lead to significant


GDPR

CONTROLLER

ROLES

Art. 4(7) Determines purposes & means of processing personal data [Why & How]

PROCESSOR

Art. 4(8) Processes personal data [What]

Controller liable for Processors & Sub-Processors

Processor liable for Sub-Processors

JOINT CONTROLLER

Rec.79; Art.4(7), 26 Two or more parties that jointly determine purposes & means of processing

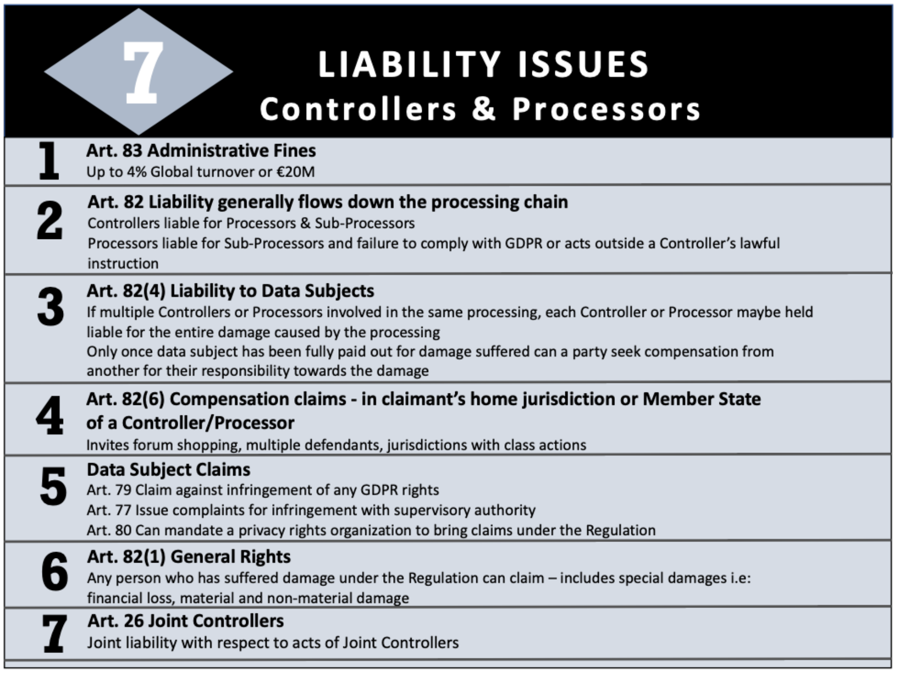
SUB-PROCESSOR

Art.28(2),(4) Processor requires consent of Controller

ICO (UK) DRAFT GUIDELINES 2017 Affirm prior 2014 guidance that deems payment services as Data Controllers exposure particularly were a payments actor is deemed to be a joint controller together with its merchants.

To illustrate the effect of liability in the event of a breach of GDPR: an incident involving 200,000 data subjects, with estimated damages of €100 per data subject translates into a claim amounting to €20 million – that is the figure that has resonated strongly with so many companies in relation to fines.

There are also contractual issues to consider. Under the GDPR, data processing agreements (DPAs) have to be negotiated with processing partners. Indemnities and liability caps are often an issue in such agreements. Care has to be taken to ensure that exposure is sufficiently covered by indemnities and that rights to recoupment of losses are not thwarted by liability caps.



7 **LIABILITY ISSUES**
Controllers & Processors

1	**Art. 83 Administrative Fines** Up to 4% Global turnover or €20M
2	**Art. 82 Liability generally flows down the processing chain** Controllers liable for Processors & Sub-Processors Processors liable for Sub-Processors and failure to comply with GDPR or acts outside a Controller's lawful instruction
3	**Art. 82(4) Liability to Data Subjects** If multiple Controllers or Processors involved in the same processing, each Controller or Processor maybe held liable for the entire damage caused by the processing Only once data subject has been fully paid out for damage suffered can a party seek compensation from another for their responsibility towards the damage
4	**Art. 82(6) Compensation claims - in claimant's home jurisdiction or Member State of a Controller/Processor** Invites forum shopping, multiple defendants, jurisdictions with class actions
5	**Data Subject Claims** Art. 79 Claim against infringement of any GDPR rights Art. 77 Issue complaints for infringement with supervisory authority Art. 80 Can mandate a privacy rights organization to bring claims under the Regulation
6	**Art. 82(1) General Rights** Any person who has suffered damage under the Regulation can claim – includes special damages i.e: financial loss, material and non-material damage
7	**Art. 26 Joint Controllers** Joint liability with respect to acts of Joint Controllers

Designations as to Data Controller and Data Processor roles need to be spelt out in agreements. Often the final contractual language reflects the relative bargaining power of the parties. Even so, the parties' own declarations on the subject can be overruled by the courts and regulators.

Knowing your partners and conducting full due diligence on privacy and security practices is a must, but this is made much harder by the current lack of any uniform privacy certification regime akin to PCI certification. This really is a big disconnect in the legislation and one that could take several years to fix.

There can also be issues as to who controls the messaging to data subjects in a data breach situation. Normally this will be the Data Controller under the GDPR and this can work against parties deemed Data Processors or Sub Processors.

This all amounts to a fairly dark and uncertain picture for payment players. There is, however, some light at the end of the tunnel. The GDPR can be regarded as a valuable, if partially flawed, piece of legislation. It has helped to make business and individuals consider the importance and value of privacy rights. If data truly is the 'new oil', then businesses cannot go around spilling it carelessly.

The regulators are not out to scare businesses. They want to see a true and sincere investment in securing and managing personal data. Companies should consider adopting a more holistic approach to privacy compliance. They need to commit from the top down to supporting best practices concerning the provision of comprehensive staff training, data mapping, responsible safeguarding and management of personal data across the business.

On the technological side, the importance of data encryption cannot be ignored. If the personal data that a company holds and transmits is fully encrypted a business' own liability can be significantly reduced. More than 95% of data breaches that reach the authorities have involved unencrypted data - a damning statistic.*

There is a substantial element of self-interest involved. The reputational damage of a data breach related to processing of data can be extremely harmful and the potential financial claims and fines might severely test a company's ability to survive. Businesses that demonstrate organized sensible practices are also likely to benefit from improved goodwill and trust with their customers.

Transparency is important and so is the realization that companies need to vet every business partner with immense care as this amounts to extending the chain of liability to each partner's business partners. In short, companies need to practice "safe business."

Many companies will find it difficult to identify themselves as just Data Controllers or exclusively Data Processors. For this reason, in the payments industry it is common for Data Processing Agreements and Privacy Policies to be drafted to take into account that the parties may be performing multiple roles with respect to the GDPR. Unfortunately, such blurring of the lines can invite protracted argument when a precise delineation of roles needs to be clarified, for instance in an actual breach situation.

Lastly, there is a dissonance for the payment industry between the GDPR and PDS2 affecting
Businesses due to different provisions relating to breach reporting. This results in having to report to a payments regulator within 4 hours of initial discovery of a breach under PSD2, and also that the payment business involved needs to make the report. Under GDPR the Data Controller is the party that should report the breach to the relevant data privacy regulator within 72 hours even when the breach affected a Processor or Sub Processor.

In conclusion, it is clear that there is no certainty on the horizon for merchant and payment services in relation to the GDPR. However, engaging fully with the spirit of the legislation and adopting such a posture across a business, should place organisations on the path to being better able to deal with issues when they arise.

** Source: http://www.breachlevelindex.com/*

Eliad Saporta
Managing Director
Coriunder

From **Rings to Pyramids**

From merchant Onboarding to GDPR requirements and working with affiliates there is no real “One size fits all” solution, each type of account (Merchants / Customers / Affiliates/ Acquirers/ Issuers) has its own set of limitations and regulatory requirements.

To accommodate all the needs of all the accounts we manage we decided to break the process into two phases – A layered approach and the Pyramid approach.

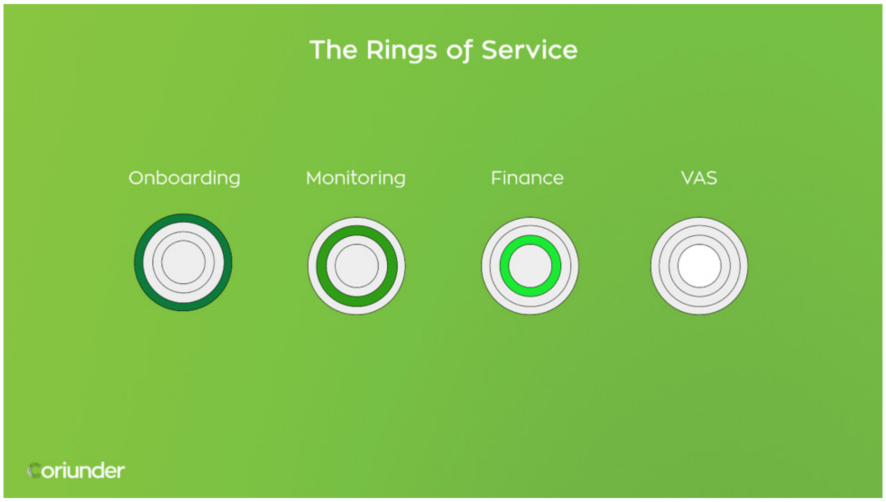
Phase One: The Rings of Service

Build the foundation of the system based on four main layers: Onboarding, Monitoring, Finance, and VAS – each layer is based on the previous one and workflows are set to run from layer to layer.

Ring of Onboarding – Managing the onboarding process of each account requires the same fundamentals: Multiple signup pages, collecting documents, client facing emails, managing consent, assigning the relevant account manager and following through the integration process.

when covering all the basics in the onboarding process you give your team the ability to take control of the internal processes required by your organization, for example: working with 3rd party vendor for additional KYC checks, we partnered with Scanovate to build custom workflows in the system that allows you to pass the data to Scanovate and apply any one of the checks they provide in their platform.

Ring of Monitoring - As difficult as it is to onboard accounts to any type of service, monitoring their activity is equally important, to keep track of the different channels and providing the tools to monitor each channel separately while still allowing full flexibility is key to the



The Rings of Service

success of the service you provide.

Transaction monitoring, limits and fraud monitoring, blacklists, API requests, cart abandonment, payment page behavior and Chargeback management – with the ability to set notifications and alerts your team will be able to get to the right conclusion when needed and take action.

Ring of Finance – Controlling your margins, another important part to the success of your service, monitoring activities is one thing, monitoring the cost and revenue coming in from each activity or interaction is as important.

Its all about the "Buy rate" against the "Sell Rate" and when working with Affiliates the "Split Rate", and that is just the start of it all, what about the "Other Fees" – the approach is that every interaction is 'Fee-able' that way you can make sure that you cover all your pain points.

Circle of VAS – More than just a Ring – It's not about just charging the fees, it's about providing more value to your "accounts" and if you can charge an extra fee for that is great. We have been saying for a while that in today's market Payment Service Providers are no longer competing on pricing but rather on the services they provide – From Global acceptance and smart routing to E-commerce tools and extensions, a wide range of API calls and more.

The Value Added Service is not just when selling to your "Accounts" its also when given your staff the tools to work more efficiently with tools such as CRM for Notes, emails, file storing, Email templates for repeatable tasks (Merchant intros, client onboarding and more), 3rd party modules and more.

Phase Two: Breaking the Rings into Pyramids of Needs

Each type of account has its own needs based on the same layered approach, with the foundations in place we focus on each type of account to give all the necessary tools to manage the day to day.

We would like to focus on two out of the six pyramids as an example of how the move from the layered approach to the pyramid translates into functionality and benefits.

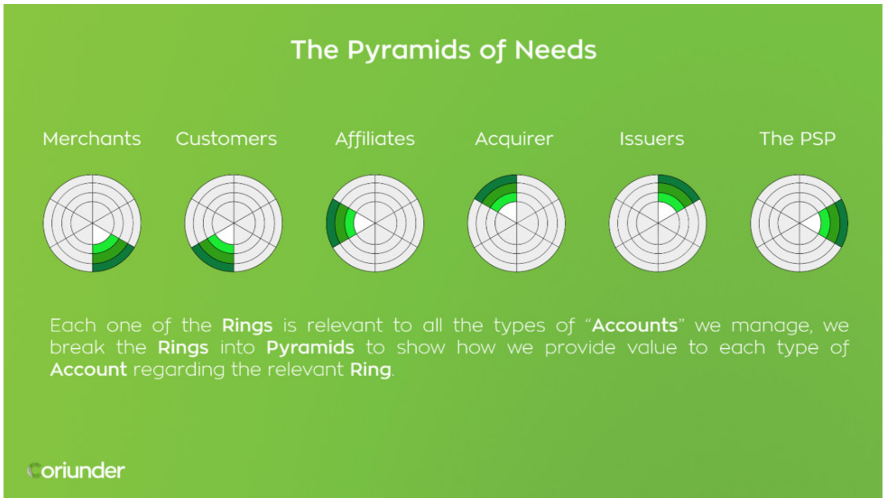
The Merchant's Pyramid of needs

The Merchant is one of the main accounts on our platform, having a "relationship" with almost every other type of account in the system, the main relationships are with the acquirers and with the customers (Cardholder/ Wallets) – to facilitate the relationships we provide tools for cost management, multiple designs for the payment pages and even landing pages and product pages allowing the merchants to share campaigns and payment links from their dedicated back-office.

The transparency between the PSP and the Merchant is important in building trust and invested a lot of our effort in building an interface for the merchants to manage their transactions and customizations.

The Customer's Pyramid of needs

The Customer account type is used in several ways, as a wallet carrying a balance, as a prepaid closed/Open loop card holder and as an app user. The system man-



The Pyramids of Needs

Each one of the **Rings** is relevant to all the types of "**Accounts**" we manage, we break the **Rings** into **Pyramids** to show how we provide value to each type of **Account** regarding the relevant **Ring**.

ages the login process, forgot password process, friend requests, account hierarchy, GDPR relevant services and more.

The relationships with issuers are the one that is playing the most significant part in the last couple of months, we built an infrastructure that allows our client to connect with multiple issuers while providing a single front-end interface to their cardholder – our unified API translates the requests to the relevant issuer and provides the relevant responses in unified format. Our clients are managing multiple card programs from one admin interface along with all their acquiring needs and fee structure.

We mentioned above the relationships with 3rd party providers such as Scanovate and at MPE we showcased the partnership we built to offer their "On-premise" solution as a SAAS service using our platform.

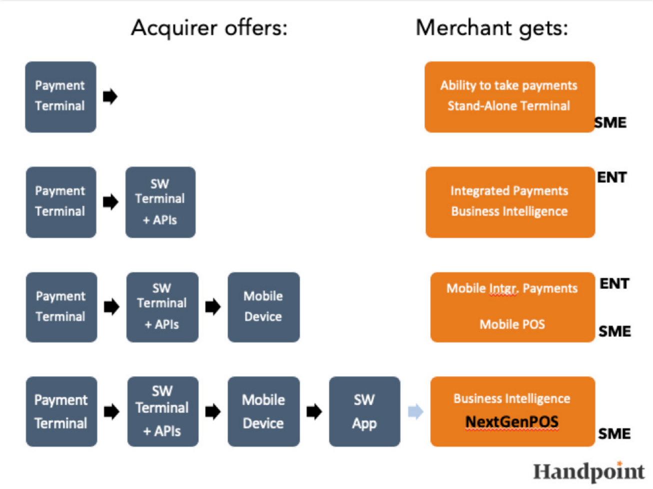
As we know, the challenges 2019 don't become smaller. A KYC solution in our days needs to work in real time, must be dynamic and must be able to be integrated in a frictionless online transaction within seconds. And this while facing regulatory conflicts as PSP2 vs. GDPR or 5AMLD vs. PSP2. Our co-op with Coriunder brings the results of our service into their backend solution - as a Coriunder client you can either access it from our interface or directly from the Coriunder backend. A management tool which identify and verify your clients, atomize the regulatory AML check within seconds, orchestra all your compliance activities in a holistic solution that gathers all data vendors into one place. You can plug in our KYC360 software on any stage of onboarding or payment process with a simple drag and drop functionality.

David Gudjonsson
CEO
Handpoint

Which comes first, Payments or Solutions?

From the dawn of the payments industry, it has all been about having the right "Payment Solutions" to offer to merchants. Now we are reaching a stage where it is all about having the right "Solutions, with Payments" to offer – and that is a game changer.
The whole payments industry is evolving fast, and so is the MPE conference, with 25% of the attendees being merchants this year (kudos to the Empiria team). Merchants are asking payment providers to stick with the trends of most other industries and provide them with complete solutions, not just parts of a solution. Almost everything we buy today, as consumers or businesses, comes in the form of either a complete solution or a solution suggestion. Buy an airline ticket, and you're offered hotel rooms, car rental, parking etc. Buy a TV online and you're offered a matching wall bracket. Buy a payment terminal/service and you're advised to call someone else in order to make it work with your infrastructure! Unsurprisingly, "solutionisation" in payments, was a hot topic at MPE this year.

How it came to this and the implications it has on merchant service providers was the topic of my talk at MPE this year. In the beginning (…after there was light and all that) there was a stand-alone payment terminal, giving merchants of all sizes the ability to accept payments. And weirdly enough – at the dawn of commercial space travel and self-driving cars – this 40 year-old-invention is still used to manage the vast majority of all payments world-wide.

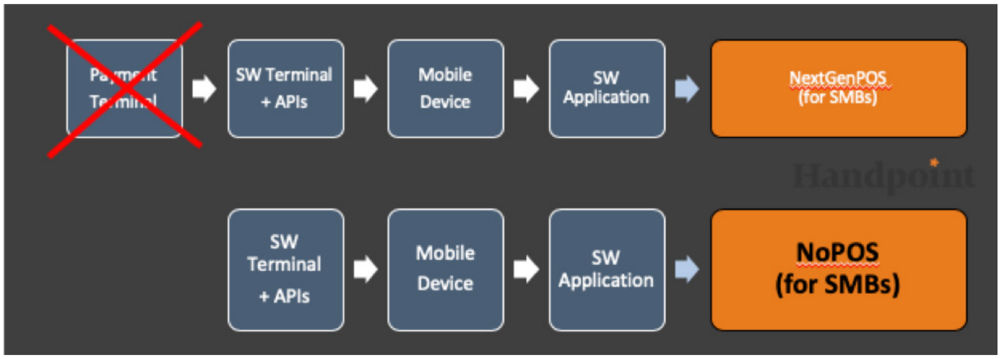


It was an honour to kick off the NextGenPOS track at MPE 2019, which in itself encapsulates this apparent evolution in payments. I am guilty of coming up with the terminology "NextGenPOS" and I remember standing on that same stage a few years back talking about the evolution in payments, mPOS and the "solutionisation" leading to NextGenPOS. And the opportunities are vast as the world is full of stand-alone terminals and 20th century cash registers are ripe for an upgrade. I stand by my earlier prediction that NextGenPOS to cash registers are what PCs were to typewriters. Now, telling of times, we have a special track on the subject at MPE.

After the payment terminal was born, a lot of exciting add-ons have happened and several building blocks have been added. Fast forward to ca. ten years ago, when a mobile device was thrown into the mix and two very exciting things happened:

- Firstly, enterprise merchants were able to set up mobile integrated payments (a.k.a. the Apple store experience)
- Secondly, Square and copycats went after the micro merchant market with a super simple mobile integrated payments offering.

What I find really interesting about the latter, is that in order to tackle the micro merchants market, the mPOS payment facilitators tackled problems that the industry had ignored: the costs and hassle of on-boarding. Now the mPOS players have set the bar when it comes to on-boarding processes and terminal pricing for SMEs and have got the industry chasing.



Then, once the mPOS players mastered the micro game, they of course didn't stop there, but added a software application on top and started offering NextGenPOS solutions to different merchant verticals. One stop shop. Once again, they've got the industry chasing.

So what comes after NextGenPOS? What other components are added to the mix? I believe the answer is two-folded:

ONE. Enhanced capability with more bells and whistles in a global setting - call it omni-commerce payment solution, or NextGen Commerce solutions (with payments!). On that topic, I must say that the Handpoint team is very proud to have won the Best Payments Award at MPE this year for our great partnership with Paysafe where we have integrated our platforms to create a global omni-commerce solution. The ability for a merchant to benefit from online and face2face payments, in multiple countries, through one provider, is fairly unique in the complex world of payments. Our partnership with Paysafe enables merchants to do just that. The MPE Best Payments Partnership Awards is an accolade for our efforts and innovation in this field, and we'll keep pushing the bar.

TWO. The hardware terminal is going away. I called it #NoPOS at MPE, for a lack of a better word, and it is about time that happened. With QR codes in the far East and PSD2 in Europe, I expect the card schemes will be pushing heavily for contactless on mobile and be tempted to get away from the (highly overrated) PIN verification. So, I expect we'll see a lot of mobile devices kissing in the near future, for the better, for both consumers and merchants.

Handpoint has been a pioneer in defining integrated payments and #NextGenPOS, from advancing the checkout experience with mobile technology to launching open payment integrations for all emerging POS platforms on three continents. We provide solutions for merchants, acquirers, payfacs, ISOs, and ISVs who are delivering on the cutting edge of payments: where customer experience and management matter, where payments are embedded seamlessly, and where mobile technology fuels growth. Handpoint's software terminal, international gateway, and terminal management system enable the future of acquiring, from mPOS and integrated POS to a future without terminals.

Handpoint. Go Mobile | Go Global

Mehdi Sabbahe
Sales & Account Manager
HPS

Payment Solutions Empowering **New Acquiring Business Models**

The modern consumer epoch is known for decisions driven by change and instability, the retail landscape is no different. Consumers are leaning more and more towards e-commerce and therefore retailers are constantly looking for new payment solutions for both offline and online operations which imposed fundamental changes on the global market.

Digital transformation has given birth to additional challenges taking shape in both new merchants and industry trends. Merchants who wish to remain competitive must embrace this change and board on a digital journey towards innovative payment solutions that guarantee convenience and security for clients, support any channel, whichever payment method and currency. The shopping habits have drastically changed over the past years which paved the way for "mobile first payment experience", with the adoption of digital wallets, the shift from POS into MPOS, thus new stakeholders integrated the value chain to provide new services.

As retailers forge ahead into 2019, industry-driven trends are evolving along the way with the standardization of offerings, the decrease in margins and competition from non-banks. All these factors embolden acquirers to branch out for new markets and seek unexplored opportunities.

Data security has been a major concern for retailers as e-commerce is evolving in an ever-changing sphere. With the rise of card-not -present fraud, acquirers should meet the terms and regulations regarding client's protection.

Large retailers have a proclivity towards building their own payment platform to support those new trends. These platforms are at the "pre-acquiring" level, which means they are connecting all consumers' touch points to acquirers.

So, what are the required capabilities to build those platforms?

Omni-channel platform is no longer an option, it's an imperative to avoid the struggle of multiple platforms once retailers have different types of purchases, be it face-to-face or online.

Large retailers across multiple geographies also need to optimize the cost of transactions based on a highly scalable solution that HPS names "Smart and dynamic routing", which implies routing authorisations and transactions to the right acquirer based on different criteria such as the type of card, the card issuer, the purchase amount, the card network, etc.

The objective of global retailers is to optimize the costs of deployment and certification by using standard protocols such as Nexo to save up costs, and facilitate the process of deployment across multiple countries.

Only in the combining of the above-mentioned requirements that such platforms can operate. Therefore, pre-acquiring platform also need to be highly available, secured and compliant with regulations.

What are the opportunities that those platforms bring to large retailers and acquirers?

1. Customer insights
Once retailers have control over such platforms, they can easily obtain an extensive overview of the customer's transactions, profile and data, while keeping customer data anonymous by tokenizing their payment means. Consequently, it is easier to analyse the spending behaviour, something that it is only accessible through these platforms.

2. Value added services
The technology behind data pooling has the potential for companies' growth. Professionals dislike fragmented systems due to the complexity of integration and deployment of value-added services (alternative payment methods, DCC, loyalty, couponing, ….). Centralizing the integration of value-added systems within one single platform will simplify deployment and provide a unified user experience for both merchants and consumers.

To address all these challenges and opportunities, HPS provides retailers and acquirers with a flexible and modular platform that relies on 4 main building blocks, a front office to manage authorizations, a back office to manage merchants (this includes merchant hierarchy, as well as merchant contracts) and merchants' transactions , a Tokenization engine to support all new payment means, and finally a personalized web portal to serve merchants and managers, fully aligned with the merchant hierarchy.

The platform supports pre-acquiring, optionally the acquiring and it is Nexo-ready.

Jeremy King
International Director, Europe
PCI Security Standards Council

Q. What are some of the payment challenges we are seeing in Europe today?

A. Within the payments industry we are seeing a huge shift in how people want to shop. Recent statistics highlight that 41% of customers would leave a store rather than wait in long queues! And 47% of UK customers carry less than £5 in their wallets.

According to UK Finance, in 2017 card-based payments overtook cash in terms of the number of transactions undertaken. In fact, cash as a percentage of all payments has dropped from 61% in 2007 to 34% in 2017 and is set to fall further to only 16% by 2027.

Q. So, what is the PCI SSC doing to address these payment trends?

A. Our focus at PCI SSC is providing standards for securing card payment data. More and more businesses are using smartphones and other commercial off-the-shelf (COTS) devices to accept and process card payments. In Europe, the overwhelming number of card-based transactions are debit, and the majority of those are contactless. Consumers and businesses love the convenience and security of tap and go. As these payment acceptance methods continue to gain adoption, PCI SSC's focus is on providing security standards for ensuring the protection of payment data, first with the PCI Software-based PIN Entry on COTS (SPoC) Standard released in 2018, which provides requirements for developing secure solutions that enable EMV® contact and contactless transactions with PIN entry on the merchant's consumer device using a secure PIN entry application in combination with a Secure Card Reader for PIN (SCRP).

And now with the development of a new PCI Contactless Payments on COTS Standard, PCI SSC is providing security requirements for solutions that enable a merchant's COTS device to accept contactless payments without the need for a dongle or other type of peripheral reader by leveraging the native NFC capabilities inherent to a COTS phone or tablet.

Ultimately, these standards will help provide a wider choice of secure acceptance options for merchants.

Q. How does the SPoC standard secure payment data?

A. The SPoC standard utilises three key factors to ensure the security of the PIN, card data and transaction in an approved SPoC solution.

1. The card data is encrypted in the PCI approved Secure Card Reader-PIN (SCRP) immediately upon entry and is never available in the clear with the PIN.
2. he payment application on the phone, PIN CVM App, encrypts the PIN data entered into the device, delivers this encrypted PIN to the SCRP where it is decrypted, formatted into a proper PIN block and then hardware encrypted before sending both PIN and Card data via the PIN CVM App to the back end monitoring system for processing. Finally, the PIN CVM App validates the security of the phone and the SCRP.
3. The back-end monitoring systems undertakes a complete health check of the process, validates all security features are in place and working correctly, and processes the payment data received.

Q. What is the next phase for PCI SPoC and the new Contactless Payments on COTS Standard?

A. PCI SSC launched the SPoC Standard and supporting validation program in 2018. Solution providers are currently developing solutions for the marketplace.

PCI SSC is targeting publication of the Contactless Payments on COTS Standard by the end of 2019. Currently we are drafting the standard as well as the derived test requirements. Following development of the standard, we will begin work on the accompanying program guide and supporting documents, which will facilitate the assessment by PCI-recognized labs and subsequent listing of these solutions on the PCI SSC website.

As part of this process, we will be soliciting feedback on these documents from the payment card industry over the next few months. This will include gathering input from our dedicated PCI Mobile Task Force comprised of more than 100 PCI constituents, and conducting two requests for comments (RFC) periods with PCI SSC stakeholders.

The first RFC period is scheduled to open in April 2019. PCI SSC stakeholders can expect additional communications from PCI SSC with information on the standard and RFC opportunities.

Q. Where can we find additional information about payment card security standards and programs?

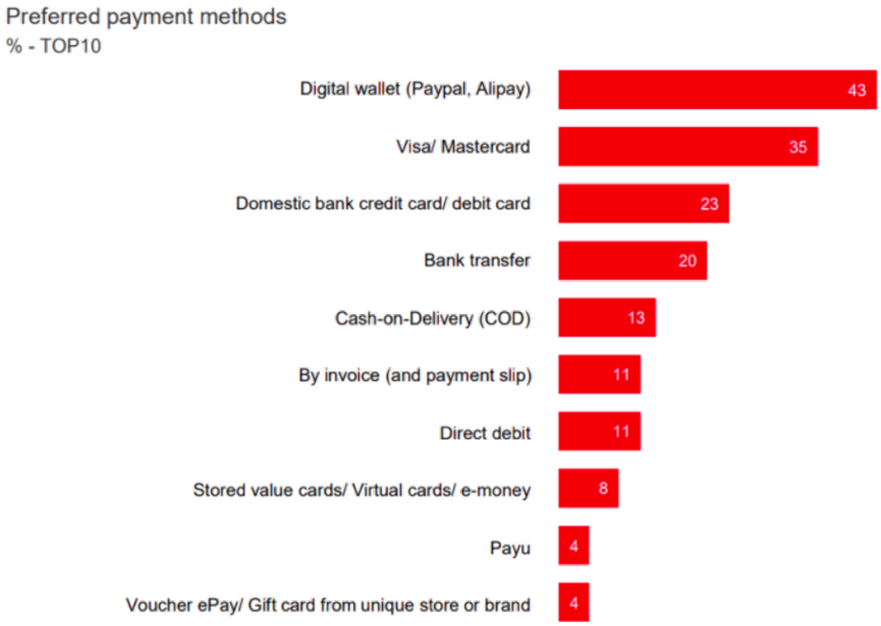
A. Payments and technology are constantly changing, and with these new standards and programs, PCI SSC is broadening the opportunity for card-based payments whilst ensuring the highest levels of security. Further details can be found on our website at www.pcisecuritystandards.org

Donald Chapman
Chief of Business Development
Modo

At Modo, we like to call ourselves #paymentsgeeks. It's actually a term of endearment around here. Because we have a love of payments, we thought it would be fun to give a little lesson around why payments are so important in the checkout experience.

Let's dig into the ABC's of Payments & Checkout, shall we?

A is for Acceptance



Accepting the payment is the beginning of the buying process. You have to accept the payment for this whole selling thing to work, right? But, sometimes that isn't as easy as it seems. Buyers across the globe want to pay using different methods from digital wallets (PayPal, Alipay), to cards, to invoicing and even cash-on-delivery.

As you continue to move globally, accepting more of these payment types becomes more important to your growing customer base. Even just in Europe, there are a whole host of payment methods preferred by consumers when comparing one country to the next.

So the lesson here? Accept the money customers are trying to give you for your goods and services in their prefered form. Seems pretty straightforward.

B is for Buying

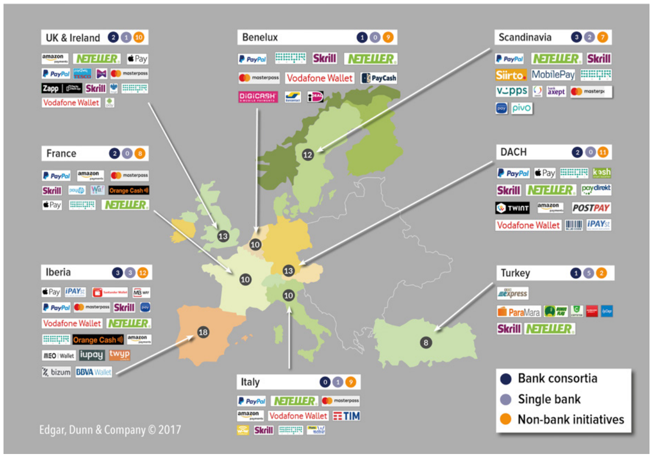
We think everyone can agree that buying is an essential piece of the checkout process. So why isn't buying made as frictionless as possible? According to PYMNTS, "Online merchants lose $147 billion as a result of transactions that consumers abandon before completion due to friction in the checkout experience." That's a number too large to ignore. And a huge part of that checkout friction is related to the payments experience.

Whether the friction comes in when your customer is required to provide details to make a payment, or what happens after they've done all that detail entry, the whole point of the online experience is make it more convenient for your customers to buy. Don't ruin all the work by offering a poor buying experience.

C is for Conversion

Oh, conversion. You get a customer on your site. They're scrolling, they're adding things to their basket, they're going through the checkout process, and then they stop and abandon their cart. What can be done to change this? In a

European Digital Wallet Landscape



Edgar, Dunn & Company © 2017

research study done by Forrester, most merchants believe that offering easy payment types is the most important factor in increasing cart conversion.

Another study done by Baymard found "the potential for a 35.26% increase in conversion rate translates to $260 billion worth of lost orders [in the US and EU]." Wouldn't it be great to get some of those billions back?

The lesson here: If your customers don't actually end up buying something, you don't get paid. Surprise, surprise.

D is for Declines and Disputes

Disputes and declines are really getting into the heart of payments so we're loving this lesson (but also hating it because disputes and declines are bad). Fixing this payments issue can have such a huge impact on your bottom line.

Riskified estimates lowering false positive declines can increase sales revenue from 3% to 30%. We have spoken to companies with billions of dollars in volume who are seeing decline rates higher than 30%. What an impact payments can make for those merchants! And when a customer get falsely declined, what are they likely to do? That's right - go to a competitor. We need to be talking more about this issue in the industry.

The other component to the 'D' section is disputes. Disputes are so hard to win and so expensive. Some merchants don't even bother fighting chargebacks. Chargebacks911 found "merchants win about 21% of disputes. This figure is less a reflection of actual guilt or innocence, and more an indicator of how difficult representments can be."

What we've learned here is: 1. You don't want to lose a good customer to a false decline, and 2. You also don't want to fight with your customers because you will likely lose (even if you win).

E is for Errors, Exceptions, and rEfunds

Errors, exceptions, and refunds cost you $$$ and lots of it!

Let's kick it off with refunds. Revolve, a cool-kid ecommerce retailer, saw returns almost as large as their net sales revenue in 2017. And they cover return shipping costs for their customers. This is insane. Think about the money it is costing them to process all of those returns.

One way to help your bottom line? Make errors, exceptions, and refunds cost less.

F is for Fraud and Fees

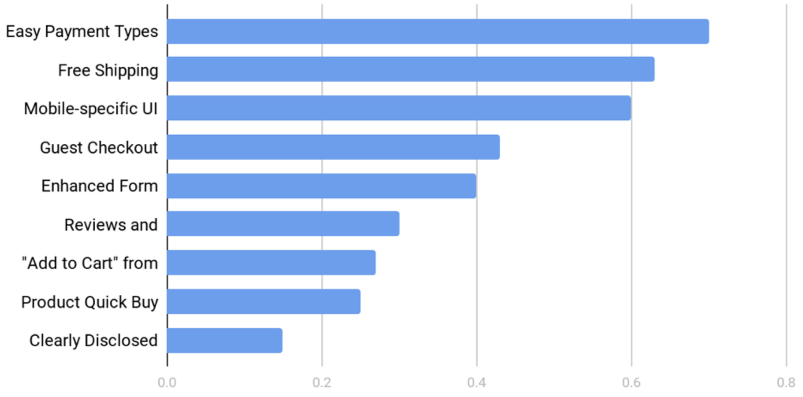
Fees for payment services are just a part of the deal. The issue, though, is that there can be a huge range in these fees and you usually don't have much control over them. In some cases, the payment fees can be larger than net profits for certain sized transactions.

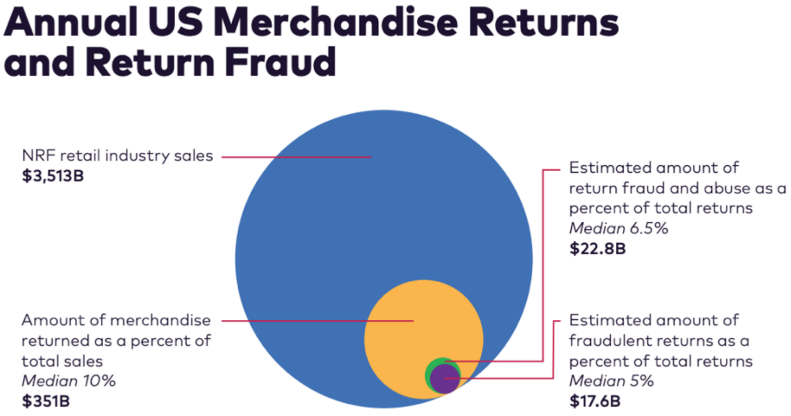
To give you a sense of the average fee size, we went to our trusty online source, Investopedia, which states "Per transaction fees vary across service providers, typically costing merchants from 0.5% to 5.0% of the transaction amount plus $0.20 to $0.30 per transaction." 0.5% - 5.0%? That's quite the range.

Fraud is another part of the deal (unfortunately). But, worryingly, even though more is being done to combat fraud, the fraud rates continue to increase. According to PYMNTS, there was a 5.5% increase in ecommerce fraud from Q2 2016 to Q2 2017.

The lesson: Fraud and fees both create friction in the pay-

"Of the following checkout features, which do you think is most important to increasing cart conversion?"




Annual US Merchandise Returns and Return Fraud

ments and checkout experience. You want less of these.

The Rundown

Impressed by what you learned? Probably not. You already knew much of that because you live and breathe ecommerce. But all we did was throw you a bunch of issues. What about the ways to solve them?

What if you could:

- Add payment services, payment methods and countries without adding complexity?
- Better understand your costs, on a payment by payment basis?
- Close more sales, by routing around "soft declines"?
- Diversify and optimize your payment service providers, for each payment?
- Easily reconcile payments, orders, and bank statements?
- Find fraud, errors, exceptions and other problems before month-end?

Intro Modo.

Through one connection to Modo's /Checkout API, we're enabling all of the providers you have or need along with all of the methods of payment you may want.

That lets us do cool things like transactional assurance. If you get a decline from one provider, we'll simply try another one. Our dashboard also gives you better visibility into your payments across multiple providers, including settlement, and allows you to switch between them based on your business rules.

There are a variety of components and benefits to our /Checkout product from Optimize and Manage to Insights and Secure. All of which enable you to simplify your payments stack. Modo gives you one connection to the entire market of payment services, across providers and payment methods.

We're proud to have some of the biggest names in payments, financial services, and retail like Etihad Airways, Klarna, 14 West, Bank of America, Deutsche Bank, FIS and Mastercard accessing payment services through our market.

Modo is here to do the most good, for the most people by reducing friction in payments. And there are quite a few ways we can help with the challenges we laid out in The ABC's of Payments & Checkouts.

Want to learn more about how Modo can help you reduce friction in your payments experience? Reach out to the #paymentsgeeks at Modo at info@modopayments.com.

Mishal Ruparel
GM, Europe
Banking Circle

Banking Circle Lending:
instant business loans for today's SMEs

My favourite place to grab a bite to eat is a little independent restaurant in Stoke Newington. They do the best middle eastern food in London, and I'm certainly not the only one to think so – the buzz every lunchtime and evening is testament to that. Their success, however, is no guarantee of continued growth.

When I spoke to the owner recently, while waiting for my lunch, I learnt that they are hoping to expand the business, purchasing a mobile food truck, but are coming up against multiple hurdles which are causing them to think twice. The problem is that a food truck is not cheap to buy, staff and run, and is seen as too risky for a traditional business loan from a bank.

It's not just launching a mobile food service which is less desirable for a business loan. Restaurants can find business borrowing for other purposes difficult too. A commercial refrigeration unit could cost £10,000, and if the fridge at a seaside café breaks one cold and rainy February, it could be tough for the business to pay to replace it immediately. Looking at the restaurant's last three months of cashflow, a bank is likely to decline a loan application.

And what about gyms? We all know they are full to bursting every January, and sometimes even into early February, with New Year's Resolutions fresh in our minds. Then they start filling up again as the summer approaches and swimsuits whisper from the back of the wardrobe. Seasonal businesses often find it difficult to get access to additional funds to help them fast-track expansion plans, whether for new branches, larger premises or adding staff and services. Even when such a business does get its hands on the much-needed loan, repayments are fixed and don't reflect the natural ebb and flow of healthy business cycles.

SMEs make up 99.9% of private businesses and employ 60% of the UK workforce – that's an astounding 16.1 million people. By 2025 SMEs will contribute £241bn to the UK economy. But recent Banking Circle research provided an appalling insight on how SMEs are currently being served by banks: over half of UK SMEs have been unable to access the cash they need in order to grow.

Some of the difficulties SMEs faced in getting hold of the cash they needed include poor rates, high fees, slow facilitation and length of loan available. A quarter (24.6%) of the SMEs said that without additional funding they would have to let employees go. 13.3% expected that the business would not survive without access to extra finance. This is a real danger to the economy, when SMEs employ such a huge number of people.

But its not game over for the SME. The good news is that payment providers working with Banking Circle can change this reality.

Banking Circle is a financial utility capable of handling non-core banking functions such as payments, FX and loans, on behalf of other financial institutions. This removes the financial burden and risk from the bank, PSP, Acquirer or other Financial Tech business, allowing them to focus on the all-important customer relationship whilst still delivering the best solutions and remaining competitive in a changing market. Banking Circle does not compete with the bank or FinTech but supports it in delivering the best service possible.

Banking Circle Lending is a new solution we have launched to tackle the growing issue of financial exclusion for businesses. Too many companies are unable to reach their potential due to slow cashflow, late payments and business cycles which put off traditional banks from extending necessary loans.

PSPs working with Banking Circle can add value to their proposition by offering fast, low-cost and flexible loans to their merchant customers. Once approved, a loan is deposited into the merchant's account within minutes and is delivered in the name and branding of the PSP, but with Banking Circle taking all the risk. From application to the loan being paid into the merchant's account takes up to 72 hours, compared with up to 60 days for a traditional business bank loan.

Banking Circle issues a virtual account in the name of the merchant. The Acquirer redirects its card funds due to that merchant into this account, and Banking Circle deducts the agreed loan repayment and settles the remainder instantly into the merchant's account. Repayments can be a fixed amount or flexible percentage, ensuring repayments mirror the ebb and flow of even the most seasonal business.

This new way of lending is transformational for small businesses across Europe: businesses which otherwise could not access loans and could not expand or may even be forced to close their doors.

Supplementing the lending solution, we recently launched a new receivables financing solution, Banking Circle Instant Settlement. This is an instant loan based on payments due into the merchant account from card takings, without having to wait for payment cycles. Imagine what this can mean for a restaurant which usually has to wait up to five days to receive its settlement funds from the Acquirer. Or for a seller waiting to receive funds from an online marketplace with a payment cycle of 90 days.

This can be a lifeline to a small business. It can also drive a new income stream for acquirers and PSPs swimming in a highly commoditised ocean, helping them to grow and stand out in a crowded market as well as changing small businesses for the better.

Working with Banking Circle, financial institutions can offer business customers access to better borrowing solutions, without having to devote in-house resources or invest in new systems development. Working with third parties in the ecosystem model championed by Banking Circle allows financial institutions to deliver transparent, easy-to-manage, flexible and low-cost lending solutions. And crucially, without risk to their own business.

Adam Bowman
Director of Partnerships
Trustly

Going all in: What e-commerce merchants can learn from the igaming industry

Adam serves as Trustly's Director of Partner Sales, managing a team focused on growing and managing Trustly's pan-European Partner network. Prior to Trustly, Adam worked at PAY.ON, where he initially helped launch PAY.ON's gateway business in the US, and subsequently managed the European sales team, based out of Munich.

When it comes to innovation, few industries lead the way quite like the igaming industry. Gaming companies' appetite for risk makes them open to trying new ideas and as a result, they tend to be on the cutting-edge of technology.

Take Pay N Play®, for example. Trustly developed this payment and registration technology in 2015, and today it has become a standard in European online gaming. Registering at a gaming site has traditionally involved filling out lengthy registration forms and then waiting days for the online casino to conduct its due diligence. But with Pay N Play®, in order to register and deposit, all a player has to do is make a deposit via his or her trusted online bank — no redirect away from the mobile gaming site is necessary, which drastically improves conversion.

From the player perspective, it's incredibly frictionless. But in the background, it's rather complex; as the player makes a deposit, Trustly extracts necessary information from the player's bank account to fulfill KYC requirements and delivers the data to the operator, who can register the player account in the background. During this step, operators can verify the player's identity and age, ensuring that he or she is allowed to play. Not only does it streamline the registration and deposit steps, but it ensures that operators stay compliant with increasingly strict security regulations.

Pay N Play® also enables instant withdrawals, so players can cash out their winnings to their bank account right away. When Trustly first introduced Pay N Play®, some operators were very skeptical. They didn't see how offering instant pay-outs to their players would actually increase deposits and ultimately build loyalty. They were worried that if players could withdraw their money instantly, they would cash out and never return. But it turns out, offering instant withdrawals had the exact opposite effect.

According to internal Trustly data, not only has Pay N Play® helped to attract a large player base quickly, but players remain more engaged and deposit over 80% more every month compared to a traditional gaming operator on average.

What e-commerce merchants can learn from the online gaming industry

So what can we learn from a solution that has revolutionized the gaming businesses? At the end of the day, players are shoppers and shoppers are players. Their behaviors are influenced by the same innate attitudes: they want to be in control of their money and they want a frictionless experience that won't disrupt their expectation of instant gratification.

Likewise, gaming and e-commerce merchants are not so different. They both strive to increase the number of purchases and to offer the most convenient and simplified processes for withdrawals or refunds. And, realistically, they would prefer to ignore the reality that their customers are asking for refunds at all. However, there is much to be gained from giving your customers — whether they are players or shoppers — what they want.

According to a recent Trustly report called "Rethink Your Refunds, Perfect Your Payments," while free returns are now commonplace, refunds have not kept pace. In fact, timely processing of refunds is a core factor affecting the customer's experience. But many companies overlook this, assuming the offer of free returns is good enough. As a result, 69% of customers report waiting four days or more for their refund.

However, the report goes on to reveal that offering faster refunds would lead to 58% of customers spending more and 56% shopping more frequently. On top of that, 95% of shoppers said they would be more loyal to a merchant that offered same-day refunds. Overall, this represents a solid uplift in revenue without merchants needing to fundamentally alter their product offerings or business model. So while free returns earn you the sale, smart returns earn you loyal customers.

A frictionless future

Clearly there are financial advantages to offering faster refunds to your customers. However, when we look more closely at the magic of Pay N Play®, the true value comes from the data that Trustly can deliver to the merchants during the bank payment process. When applied in an e-commerce perspective, the potential can be equally transformative.

Imagine shopping on your favorite brand's website, and when it's time to check out, you simply make a payment through your online bank and you're done. No need to fill out a long form with your shipping details. Because Trustly can fetch that data during the payment process, the merchant can pre-fill the shipping form, which the shopper can confirm with one click. Or the merchant can even create a unique shopper account, but there's no need to remember a username or password because shoppers verify themselves through the payment. The result is a much more frictionless checkout experience, which benefits both the shopper and the merchant.

But why stop there? Trustly's latest innovation, In-Banner Pay N Play®, takes things a step further and puts the streamlined payment experience into a banner, which can be distributed across the internet. Imagine scrolling through your favorite fashion blog and you see a banner advertisement for a beautiful pair of shoes. You can buy them by making the payment from directly within the banner (hosted by the merchant) and never even need to leave the page you were surfing. It's an e-commerce experience that meets shoppers where they are, rather than redirecting them to a new page. It finally takes e-commerce into the world of impulse buying.

When e-commerce merchants, like gaming operators, start to view payments not as an obstacle but as an opportunity to increase conversion and streamline the shopper journey, everybody wins.

Tristan Chiappini
Head of Account Management
PPRO Group

Customer **shopping trends** of tomorrow

Change is happening!

Customers don't refer to themselves as 'ecommerce shoppers' or 'face-to-face shoppers'. To them it's just shopping. Similarly, terms such as 'cross-channel', 'multi-channel' and omni-channel' are starting to sound somewhat outdated – they still focus on the "channel". Commerce is moving from being channel-centric to being increasingly customer-centric.

Enabled by intelligent systems and insight, customer-centric commerce personalises and customises the experience depending on – you've guessed it – you the customer. After all, we all have different considerations and needs when we buy our morning coffee, pay our gas bill, order a take-away or purchase a second-hand car. This difference is amplified across different markets, generations and contexts.

Payment fragmentation

How and why people buy depends on so many factors. How and why they pay depends on a whole host more. Our research shows that while commerce is becoming more global, payment is becoming more local.

The internet has no boundaries, customers search for a wider selection of goods and lower prices. And this search often leads outside their home countries. The amount spent on retail online in 2017 was around $2 trillion, according to Forrester. With 60 percent of the world's population expected to be online by 2022, more than 20 percent of B2C ecommerce will be cross-border, Forrester estimates.

This creates the first of many natural tensions for customer-centric commerce. Far from consolidating, payments are fragmenting. Global payment brands such as Visa and Mastercard account for only 25 percent of global ecommerce payments. This will fall to 15 percent by 2021 according to the recent Worldpay Global Payments Report.

There are more local payment methods than ever before – in our experience there are around 350 significant LPMs worldwide. These follow customers wherever and however they shop, at home or abroad, online or in-store. Acquirers, payment service providers (PSPs) and merchants must accept that unless they have the right payments infrastructure and can localise payment, basket dropout rates will rise and they will miss out on sales.

For example, if you are selling online in the Netherlands or trying to appeal to Dutch e-shoppers, then accepting iDEAL is a must. Almost 60 percent of online purchases are made via this bank transfer method. That equated to roughly 378.2 million transactions (more than 30 million per month), totalling €33 billion in 2017, the last full-year for which statistics are available.

It is a similar story in Brazil with the popular local cash-based payment method Boleto Bancário. This accounts for nearly 25 percent of online payment transactions. At check-out, the customer selects Boleto Bancário, receives a unique reference for their payment, and then pays this in cash at various locations like ATMs, banks, kiosks, post offices, retailers and convenience store, or supermarkets. This offline way to pay for online purchases is not unique to Brazil.

Cash-based or cash-on-delivery type payments are prevalent worldwide, for example in Japan with Konbini convenience store payments, OXXO in Mexico, PayPoint in the UK and many many more. Payment habits are strongly national. They have developed over time and are formed by various cultural, political, economic, generational and technological factors. In some cases, the preference for locally preferred payment methods is amplified by the consumer's unease with shopping cross-border at a merchant located outside of their home country – do I really want to share my confidential payment details like card number with a merchant I don't know? Those wishing to expand internationally need to consider national payment differences.

Back-end complexity

Payments have a key role to play in enabling simpler, smarter, more customised customer centric shopping experiences.
But therein lies the second natural tension. Greater personalisation and simplification on the front-end – allowing customers to pay anyone, anytime, anyhow from any device or funding source – creates greater complexity on the back-end.

A duck analogy is apt. On the surface the duck glides along serenely, while under the surface its legs kick furiously to propel it forward. To consumers, if everything goes right, payments appear to happen seamlessly on the front-end as if by magic, yet the right payments, often complex, infrastructure at the back-end is essential to delivering this.

Acquirers, PSPs and merchants differentiate their offering by focusing on the front-end customer experience. So, they need the right partners at the back-end to take care of payment complexity. The need for local payment expertise as well as a centralised, value-adding hub for payments has never been greater.

The commercial opportunity in payments is happening around the transaction. Switching packets of data from one place to another became commoditised long ago. As processing fees continue to decline, revenue will come from new ways to monetise data and value-added services. This may be loyalty, funds collection, speedier settlement, reconciliation or FX.

This is where smart partnerships and new collaborative models come in. The payments industry has a long tradition of outsourcing, partnering and collaborating across a fairly wide set of organisations. If anything, outsourcing and specialisation within the industry are only set to intensify.

For example, people talk about APIs and setting up API calls to different systems. But it's a massive burden of PsP's development resources to keep all of these API libraries up-to-date if they were to go it alone. This is time they could have spent delivering new products and services to their merchant customers. Then there's real-time settlement to merchants. But it takes a lot local expertise and time to optimise systems and infrastructure to collect, reconcile, consolidate and pay out via bank accounts in different countries. It may be better, faster and cheaper to outsource such back-end tasks to a specialist partner.

In summary

As commerce moves from a channel-centric to a more customer-centric model, personalisation and customisation will be key. This will be enabled by intelligent systems and supported by the right technology, infrastructure and partnerships. Payments will play a central, enabling role in driving simpler, smarter and more customised experiences.

Acquirers and PSPs help their merchants to increase reach and make customer journeys smoother. However, back-end complexity is growing, particularly with the globalisation of digital commerce and localisation of payments. PPRO as the payment professionals enable local payment on a global scale across 175 countries and help our commerce customers to increase reach and make customer journeys smoother. We use our local expertise and global network to process, collect, reconcile, consolidate and settle – all under one contract, one integration and one platform.

Rahul Pangam
CEO & Co-Founder
Simility

Making Data a Competitive Advantage: **Fighting Fraud with Big Data Analytics**

The global e-commerce market has never been more competitive. Emergent business models are transforming the way businesses and customers interact, and disruptive technologies are opening new avenues that enable rapid innovation. At the same time, the nature of today's digital-first environment requires organizations to balance rapidly evolving fraud, heightened competition, regulatory scrutiny, and changing customer behaviors.

Each competing priority has introduced a new layer of complexity for businesses. Firms are reacting in ways suited for their customers while meeting risk tolerances and allowing for constant innovation. As the landscape has evolved, point solutions have emerged to meet the changing fraud and risk patterns. These solutions may have worked in the past, but they have become ineffective against rapidly evolving fraud.

Businesses need a solution that provides a holistic view of the end customer and is flexible to changing needs and evolving fraud. Success is not dependent on how much information is available but how it can be harnessed to gather meaningful insights. The ideal solution protects against changing fraud and provides tools to harness the available data effectively.

Simility, a PayPal Service, provides real-time risk and fraud decisioning for global businesses operating in a digital-first, post-breach world. Simility's Adaptive Decisioning Platform provides a 360-degree view of the end customer and is flexible to adapt as fraud evolves. With Simility, businesses can leverage the power of big data and clear-box ML, to help ensure that they are protected against the latest threats.

Meirav Peled
Partnerships Director
Riskified

Differentiation and monetization - how new products and services are reshaping the payments landscape

Ecommerce in Europe experienced double digit growth rates over the past five years, and according to a recent Edgar, Dunn & Company study, this trend will continue into the next decade. With a new generation of omnichannel shoppers who want to shop anywhere, anytime and don't want to be delayed for even a minute, it's clear the growth is customer driven. This is, of course, great news that brings immense opportunities, not only to merchants, but to the entire ecosystem: PSPs, banks and payment platforms.

Customer demand is changing the way online merchants are conducting business, which is also driving PSP offerings. Broadly speaking, customers today expect three things from their retailers:

- Extreme convenience
- A personalized experience
- Customer service

While some shops already meet these expectations, according to Perry Kramer, a senior VP with BRP Consulting, only 7% of retailers are allowing customers to start the sale anywhere, and finish it anywhere, with another 50% planning to implement this in 3 years.

PSPs must facilitate the changes in the arena in which merchants operate. Are you offering various payment methods tailored for different geographies, currencies and an online dashboard? And are you providing a fraud management approach that is effective across all channels? Can you accommodate different regulations?

So what kinds of services can PSPs offer to optimize the shopping journey and to help merchants grow? Some examples include account protection to prevent sophisticated fraud attacks, and alternative payment methods to help optimize conversions and overcome problems like bank declines. Another important element is helping merchants adapt to regulations, like PSD2.

According to Paul Rodgers, chairman of Vendorcom, which connects seekers, solvers and shapers in the European Payments Community, when PSD2 regulations go into effect on September 14th, merchants may see as many as 30% of their transactions declined. And this is critical - because one side of getting PSD2 ready is raising awareness. When customers are not expecting change and don't understand the reasons for it, they are more likely to resist it.

To counter this, PSPs and banks that implement Strong Customer Authentication will need to educate their customers about the changes to the shopping journey, and the reasons behind them.

The other side of getting ready for PSD2 is making sure you're prepared technologically. First – make sure your performance (as PSP) is resulting in the lowest chargeback rates. This will allow you, in turn, to minimize the friction at checkout and invite the best merchants to join you. Then – use advanced technology and machine learning to ask for exemptions, pushing more transactions to Transaction Risk Analysis (TRA), and avoiding unnecessary friction.
This will ensure your customers receive a seamless shopping experience - something they have come to expect. So now, you are actually turning the security regulation into a new business opportunity.

François Lecomte-Vagniez
Advisory Facilitator
SPA Retail Workgroup

IoT Payments: addressing the protection problem

The proliferation of interconnected IoT devices offers exciting new opportunities to develop payment applications – in the home, on the move and in a wide range retail, automotive and industrial environments. But a lack of standardization, slow adoption in the financial sector, and a complex technology ecosystem presents considerable challenges that threatens to stifle innovation and market evolution. SPA investigates.

1. Introduction

While market projections differ – from Gartner's much cited 50 billion connected devices by 2020, to IHS Markit's rather more conservative 30.73 estimate – there's little doubt that the Internet of Things (IoT) is a massive and growing opportunity for payment services.

At the same time, the financial services sector has been slow to embrace IoT payments. To date, the sector has been more focused on mobile applications and wallets. This is slowly beginning to change. New use cases and commercial IoT applications capable of initiating remote payment are certainly emerging, including smart (voice-enabled) assistants and in-car dashboard systems. But the pace could be accelerated.

There are significant security risks that must be addressed if this is to happen. According to security firm, Symantec, the number of malicious attacks on IoT-enabled devices grew some 600% between 2016/17. IoT is certainly a large and growing target, and with personal data 'gold' on offer for successful hackers, there's every reason to assume attacks will continue to grow in volume, ferocity and sophistication.

This shouldn't come as a surprise. As IoT becomes a ubiquitous part of everyday lives, we're exposing every greater amounts of sensitive, personal and financial data to a host of semi (or completely) autonomous, connected devices. As consumers, it's almost impossible to know whether our connected cars, smart homes and healthcare systems are adequately protected – particularly as a new crop of immature application developers and device manufacturers appears. Added to which, in many use cases, the payer is not physically present. The authority to initiate the payment is therefore delegated to the device – which poses its own set of issues.

However, while broadening the list of connected 'things' certainly broadens the risk, this is by no means a good reason to put the brakes on change. Indeed, where payment is concerned the opportunities are many. SPA believes we should push ahead, but do so with caution and a
better understanding of how to protect these internet-connected devices to minimize the risk of attack and fraud.

2. The potential of IoT payment

One of the big 'customer experience' wins of the widescale drive to IoT is payment. In the automotive space, our connected vehicles become the payment instrument for a range of services including buying fuel, paying for tolls and parking, and multiple drive-thru retail scenarios. At home, IoT is opening up a host of pay-per-use payment models linked to the consumption of water and energy utilities, for example. We're already familiar with payment-enabled in-home smart assistants like Amazon's Alexa or Google's Assistant to buy music. There's a lot more to come.

In the retail environment, for example, payment options – from app-enabled purchasing to contactless payment on wearables – is eliminating friction and improving buying experiences. While in financial services, embedded payment options are not only facilitating person-to-person payments and payments in unattended environments, they are driving the development of more accurate financial risk management systems (by capturing information from IoT devices and networks).

These examples barely scratch the surface of what is possible in an increasingly connected world. But, irrespective of application or operational context, they all have one thing in common: data. Whether user-directed or fully autonomous, IoT devices (and particularly payment-enabled ones) generate, store and process huge volumes of sensitive data.

Today, it's at risk. And not just from cybercriminals intent on monetizing stolen data or creating havoc by initiating fraudulent payments. Corporations are also facing more regulatory pressure than ever before to effectively and securely manage (and ethically leverage) sensitive IoT-derived data.

Governments and payment regulators certainly have an important role to play promoting the design and deployment of secure IoT solutions. So too, banks and fintechs have a role in developing and demonstrating the viability (and security) of payment IoT applications.

3. The importance of the network

This is not just an applications issue. Connectivity is crucial too. Last year, wireless IoT received a major boost with the commercial launch of Narrowband-IoT (NB-IoT) networks – part of the Low Power Wide Area (LPWA) category of communications. NB-IoT makes it considerably more commercially and operationally viable to connect low bandwidth devices, via a SIM card, to a network – particularly those in hard to reach, rural or remote locations.

Giving impressive power efficiency, NB-IoT devices can run on batteries for up to ten years in the field, while the devices themselves can be built cheaply – for under $10. With this kind of price and performance, we'd expect to see significant deployments at scale in 2019. Added to which, the arrival of 5G through 2019 will be important - particularly for higher bandwidth applications.

4. Exploring the protection imperative

At the most fundamental level, IoT payment security poses a volume challenge – both in terms of the number of devices and the diversity of use cases. The more connected devices on the network – particularly if they are poorly protected – the higher the chance that one or more could be compromised by the latest mutating malware. Not only are devices designed to be easy to access remotely, they often lack the processing power and memory to support conventional security approaches – particularly in terms of managing the regular software updates required by today's signature-based AV approaches.

As above, the diversity of devices and platforms is also an issue. We're still in the Wild West of IoT deployments when it comes to many payments use cases. Securely embedding payment into IoT devices, and then doing the same with platforms as diverse as connected cars, smart meters and virtual assistants, creates a slew of design, integration and lifecycle challenges – from remote software provision to regular firmware updates to secure those IoT devices with long lifetimes. Moreover, devices need to be able to monitor and report on unauthorized access attempts – so future attacks can be blocked, or compromised devices isolated.

The core principles of IoT security are simple: protecting the physical smart devices and the network that sends and receives data online to and from authorized components. The operational reality is rather more complex. The IoT technology stack includes network infrastructure, IoT devices, cloud platforms and databases, decision-making (and self-learning) processes, communication networks and so on. Added to which, back-compatibility with existing payment systems, delegation to the IoT device, payment credential management and strong customer authentication implementations are all required (and challenging) in the payment context.

This complex environment is difficult to monitor and control with a robust certification process. Plus, the multiplicity of attack points that cause data leakage, and the lack of understanding of how to apply security controls in a payments environment, are major issues.

It's not only about the technology. The protections (and regulations) required for healthcare-based IoT systems are clearly different from those in the payments arena. Getting security right in every operational context not only requires a lot of hard technical thinking, it also need a deep awareness of the regulatory landscape in each case. The constraints posed by the General Data Protection Regulation (GDPR) and upcoming e-Privacy regulations in the European Union and beyond are a case in point.

5. Attack scenarios in the payment context

5.1. IoT administration system compromise

The compromise of an IoT administration system grants the attacker access to all the assets (devices, networks, gateways) under the control of that administration system.

The attacker is now capable of performing a range of nefarious actions including extracting confidential information, creating malfunctions or directly affecting the behaviour of the IoT environment. Since a compromised administration system leads to several assets being compromised over a long period of time and without being detected, the impact of this attack can be critical.

Current Payment Systems Security Architecture is designed with multiple control points that are well adapted to the characteristics of a limited number of certified acceptance points (i.e., terminals) using certified products (i.e., payment cards). Therefore, the integration of IoT systems may be difficult due to the scalability challenges for the security infrastructure.

5.2. Value manipulation in IoT devices

The manipulation of calibration parameters established for the sensors allows undesired values to be accepted when they should not – an issue that poses severe threats to critical systems.

In this attack, the sensor processing and knowledge model levels of the control system of an industrial robot in a factory is targeted. In payment systems, the attack targets Real-Time Risk Management Systems in payment networks authorization computing facilities.

5.3. Botnet command injections

A botnet is a network of automatic devices that interact to accomplish some distributed task.
The attack entails the exploitation of some vulnerability inside a device to inject commands and obtain administrator privileges, with the purpose of creating a botnet made up of those vulnerable IoT devices.

Due to the characteristic interconnection of IoT devices and their poor configuration, carrying out such an attack is (at least in theory) relatively simple. Unsecure IoT constitutes vulnerable entry points to payment systems. Command Injection may include fake payment authorization requests/ responses.

5.4. Designing countermeasures

What then is the solution? The first step is to fully understand the limitations of the IoT device – its lower computation power, the constrained communications channels, and the integration challenges of the diversity of environments and platforms. It is also necessary to take into account the certification vs unitary cost for payments in this IoT context.

Added to this, applications developers, payment providers, device manufacturers and integrators must also be aware of the security constraints. These include the need for authentication at scale, the multiplicity of attack points as well as the need to provide security beyond the perimeter of the system. Encrypting data at rest and in transit on the network is important too. There are also some lightweight cryptography standards that fall under ISO/IEC 29192 that can be used to reduce impacts on device performance in the NB-IoT environment.

Biometrics are playing an increasingly important role in securing IoT. We've seen fingerprint biometry become ubiquitous for Apple Pay and Google Pay solutions, and now the schemes and banks are adding match-on card biometrics to the next generation of smart payment cards.

Indeed, Visa sees a future where consumers will be able to swipe their hands over IoT-connected terminals without the need for a payment card, watch or any other device. Already its Visa Ready program provides a path to secure payment functionality in cars, wearables, household appliances, retail environments, and more. In this growing ecosystem, device manufacturers can look to approved Token Service Providers (TSPs) to enable tokenized payment functionality in IoT devices.

Similarly, the Mastercard Engage program offers solutions to help manufacturers of IoT devices more easily and quickly enable their devices with secure payments.

Looking beyond the Schemes, we have seen significant national public administration initiatives to harden IoT against cyberattack. A recent example is the proposal by the European Commission to strengthen and expand the European Network and Information Security Agency's (ENISA) mandate by addressing certification and standardization of ICT products, as well as wider plans to increase cooperation relating to preparing and addressing cross border cybersecurity challenges in Europe. Similar work is happening in the UK, with the Government here promoting secure-by-design principles and the development of best practices in the design of IoT systems.

At present however, there remains no specific financial industry standardization initiative for IoT-enabled payments or security architectures. Both of which are critical to drive development and adoption of a broad range of IoT payments applications and services.

More work needs to be done across the IoT ecosystem to enhance and extend security –whether that be new device and user authentication approaches, securing payment account information, or the wider adoption a rapidly evolving tokenization infrastructure.

SPA is exploring these and other approaches to securing IoT-enabled payment in its Workgroup program.

If you are interested in joining the SPA Retail Advisory Council, click here: https://www.smartpaymentassociation.com/index.php/about-us-smart-payment-association/join-us-smart-payment-association

Francis van den Bosch
FinTech Advisory
TD Shepherd & Co

Diderik Schonheyder
Managing Director
Schonheyder & Associates

Increasing Revenue From Acquiring and PSP Activites

Background

Acquirers historically have mostly focused on providing card payment services (acceptance of international and domestic card schemes) to merchants. They provided "stand alone technology" (pos-terminals) to make things work. Integration with in-store technology was limited to receiving total purchase amounts.

With the advent of e- and m-commerce, the Payment Service Providers (PSP) have developed a range of payment methods for use in the online world. These payment methods were set up to serve a variety of merchant and consumer segments, including the option for payment without a card. Around the world and in Europe this evolved based on which geographies their merchants wanted to cover. Their business keeps growing thanks to many types of e- and m-commerce.

Why the historic focus leads to major opportunities for new revenue streams being unaddressed

Especially in classic acquiring activities margins have become very thin. This may be less of an issue for PSPs, but also here the competition is rapidly increasing. For both acquirers and PSPs new revenue opportunities are welcome, if only to keep up the profit growth of the past. For example, in recent past we have seen the introduction of Dynamic Currency Conversion. However, as the Euro area expanded, and the consumer became more educated in currency exchange rates this could not be the only acquirer/PSP service addition.

Merchants, like most organisations, will be happy to pay for solutions that answer their problems. Also, as can be seen in the market, merchants are increasingly likely to have both physical and internet-based outlets. Acquirers and PSPs are uniquely positioned to help merchants deal with the following issues (not necessarily in order of importance).

The need to accept "all payments"

More and more merchants are active in a large variety of channels, from classic stores to various types of e-commerce. This trend will only grow in the future. Their customers expect that they can use the same payment methods in all the channels that the merchant is active in.

This creates major opportunities for parties that want to provide the merchant with a full range of payment methods in both the classic and new channels.

This approach will also deal with the expected further "proliferation" of payment methods that are made possible with PSD2 using different technologies such as chip, QR code, contactless and mobile.

The need to know your customer and for One-to-One communication (with reduced emphasis on mass marketing)

Merchants, facing the decreasing efficiency of traditional media, have a strong need to identify their customers and to understand their purchase behaviour. This regardless of the channel through which the customer arrives. The need exists both at the moment of contact with the customer and more generally when historical data is analysed and appropriate measures are taken.

Today, only very large merchants with their own customer card and loyalty programs can satisfy this need across channels. Some merchants may have this for their e-commerce channels but then often there is no connection to the in-store sales channel.

By and large, for the bulk of merchants, there is an unaddressed need here.

The data provided by payment methods, if processed in a GDPR compliant way, can provide important steps towards solutions. Acquirers and especially PSPs are uniquely placed to provide a solution because of their existing relationship with the merchant.

The need to recognise the customer

A merchant can resolve this through creating or joining a loyalty program. Creative start-ups such as Izicap and Yoyo Wallet now offer new ways to use data derived from the payment methods used by the customers. These solutions could be used by the acquirers and PSPs to better serve their merchants, but again these are only looking at the payment amount, not the basket content.

The need to make payments a part of the overall customer interaction process rather than an isolated stand-alone event

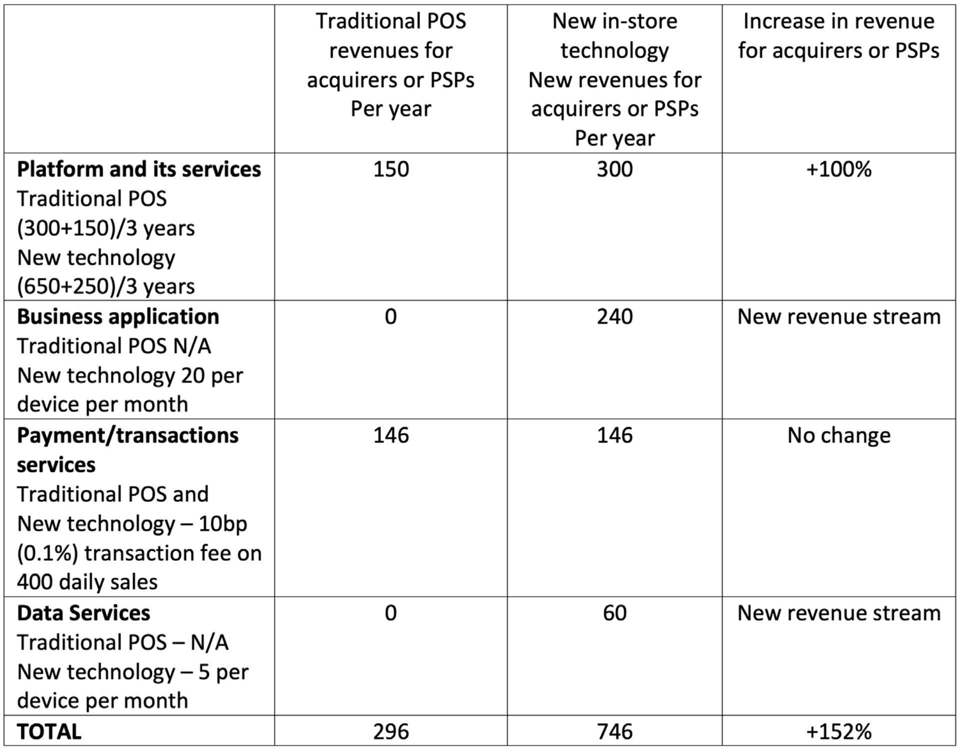
Many merchants are investing in in-store technology that supports their sales staff in becoming commercially more effective and productive.

This takes various forms depending on the sector the merchant is in. Generally, the following functions are considered: check CRM data, view customer history, find product information, check inventory, communication with back office and arrangements for financial services including offering insurance and credit.

Ideally, this in-store technology can be used in both fixed, mobile and e-commerce functions.

The need for rethinking the in-store technology and to integrate all the functions that merchants require

Acquirers and PSPs can start offering complete packages that address the merchant needs and thus have the opportunities for significant new revenue streams.
In-store technology is now becoming available from several vendors such as Verifone, Ingenico, and Aevi. Also, a very interesting solution is available from a Paris based



	Traditional POS revenues for acquirers or PSPs Per year	New in-store technology New revenues for acquirers or PSPs Per year	Increase in revenue for acquirers or PSPs
Platform and its services Traditional POS (300+150)/3 years New technology (650+250)/3 years	150	300	+100%
Business application Traditional POS N/A New technology 20 per device per month	0	240	New revenue stream
Payment/transactions services Traditional POS and New technology – 10bp (0.1%) transaction fee on 400 daily sales	146	146	No change
Data Services Traditional POS – N/A New technology – 5 per device per month	0	60	New revenue stream
TOTAL	296	746	+152%

All numbers in Euro.

new start-up called Yello. Its mission is to build a set of simple tools for all in-store services and sales.

In summary, the new in-store technology provides products and services from one device. Yello has a few different models based on screen sizes. The device can be deployed both in mobile and fixed mode and combines all the business requirements and all payments options for the merchant. One of the challenges is of course to be payment industry compliant and the Yello device:

- Is certified for EMV, PCI PTS and all payment systems including direct debit;
- Handles contact and contactless, chip cards including ID cards, magstripe, QR codes, barcodes, e.g. for loyalty cards and RFID tags;
- Can run any business application the merchant desires;
- Can be used as a communication tool for staff and can be "driven" from a distance;
- Can itself be the ECR or alternatively can connect to an ECR;
- Can easily connect to another in-store technology.

With these new in-store technology platforms, the merchant's staff can run a complete omnichannel sales process with the one device that has the capability to run many applications and can have access to a number of back office functions, while it is certified to handle all payment options.

The need for a business case – examples of revenue share for acquirers and PSPs

It should be noted that although the below table looks at the increased revenue that acquirers and PSPs should be able to receive, this new technology environment also provides significant scope for the merchant to increase its turnover. Due to the variety of merchant types, it is not practical to show this in this table. This should be done when working with individual merchants.

MPE 2019 **Media Coverage & Blogs**

MPE 2019
setting the state of commerce payments industry through knowledge

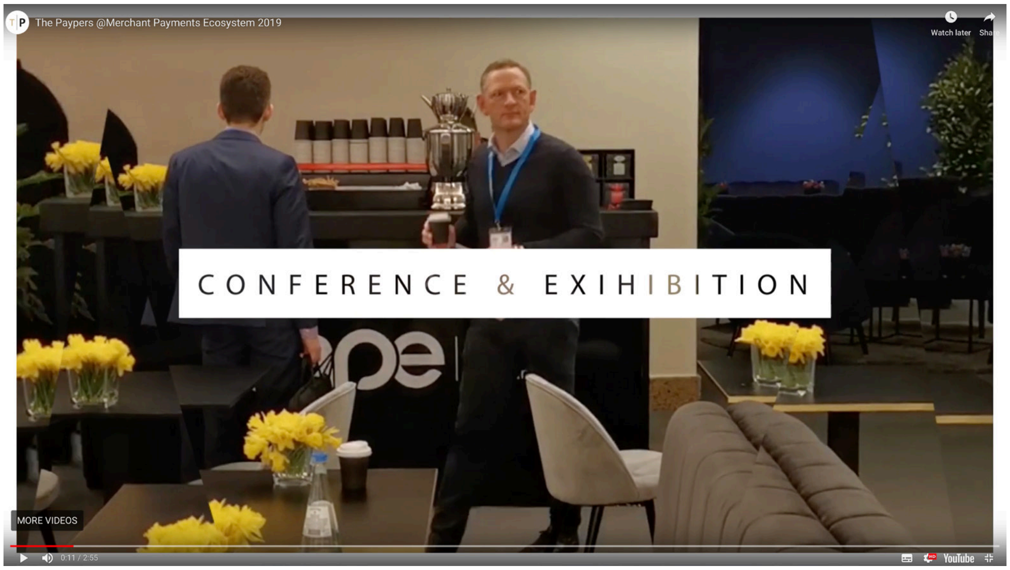
As a key media partner of the Merchant Payments Ecosystem, this year we also attended this payments-focused conference. Here are our key takeaways

PSD2 and Strong Customer Authentication - still great influencers over the payments landscape

THE PAYPERS

We may definitely extract three keywords from the MPE 2019: PSD2, SCA and customer experience. These three topics are perfectly intertwined, since SCA, which is part of PSD2, targets the end consumer. The impact of SCA worries both solution providers and merchants, as a new layer of security might affect the frictionless customer experience that everyone has fought to achieve. Some experts believe that as long as SCA will imply biometrics, there will be no friction whatsoever. As Steve Cook, VP Business Development at FaceTec, mentioned in his presentation, the improvement of facial recognition technology is going to pave the way for more easy-to-use and secure biometrics technology.

What does SCA mean for payments? Not that much for MOTO (Mail Order/Telephone Order) payments, direct debit, Merchant Initiated Transactions (MIT) and anonymous prepaid. Not that much for low value, low risk, and recurring transactions (on the same value) either. For the rest, there is a significant concern when it comes to payments acceptance. According to Martin Sweeney, CEO of Ravelin, smart technology can provide exemptions, step-up authentication and data to issuers in order to address the payments acceptance. Merchants are urged to use an acquirer with low fraud rates, outsource their Transaction Risk Analysis (TRA) and to use 3DS2 for the least bad customer experience.



Switching to out of scope payment methods might be a solution to avoid SCA, however, it very much depends on the business model of each organization. MOTO payments, for instance, are relevant for food delivery, but for other types of merchants, this method could involve even more friction than SCA might bring. We should watch this space, to see if out of SCA scope payment methods will be more embraced by the commerce businesses. Nevertheless, payment solutions providers are strongly encouraged to consider alternative payment methods with more predictable user experience. Whitelisted merchants will be exempt from both 3D secure and SCA. In addition, merchants should actively prompt whitelisting into the checkout flow, collaborate with the issuer and whitelisting providers and/or find an acquirer that can apply Transaction Risk Analysis (TRA) exemption. These remarks belong to Martin Koderisch, manager at Edgar, Dunn & Company.

Innovation drivers

The SmartPOS seems to be a disruptive element in the payments industry, opening the door to innovation, as Julien Sarat, MD at Spire Payments demonstrated in his presentation. The technology behind it will leverage a highly intelligent gateway architecture, providing new growth opportunities for banks, merchants, and acquirers. We should be thankful to smartphone developers, since the smartphone paved the way for SmartPOS, and now, drop-in replacement costs from a smartphone overlap, which means that SmartPOS might become affordable to any business.

Modern solutions for payment acceptance don't involve too much hardware, but manageable and scalable methods. Sam Shawki, CEO of MagicCube, presented the PIN on Glass/Mobile that will allow both micro merchants and large retailers to use cost-effective mobile POS, in order to create a seamless experience for merchants and consumers.

"The payment terminal is giving way to payments taken directly on consumer off-the-shelf (COTS) mobile devices. The card schemes are driving towards a contactless future, and we'll see soon a lot of smartphones kissing each other"
David Gudjonsson, CEO, Handpoint

The innovation pace walks across cash. A study conducted by Juniper Research has revealed that 75% of UK adults expect all retail outlets to accept payment methods other than cash. Windsor Holden, the representative of this company, also revealed different use cases where card payments can be used with mPOS devices: music festivals, taxis, mobile businesses. Moreover, both consumers and businesses can see the advantages. The first doesn't need to carry cash, the latter may benefit from these operations that are highly dependent on cashflow to remain in operation.

According to the research company, the growth in this space is driven by:

- accessories shipments expected to increase from 14 million in 2018 to 29 million in 2023;
- PayPal acquisition of iZettle key in strategy to develop seamless offline/online experience in multiple

markets;
- traditional POS providers (Ingenico, Verifone, PAX) gaining traction in selected markets.

If we look at the US market, another research conducted by Electronic Transactions Association has shown that 73% of the population has a smartphone; of those, 11% use mobile payments, with Apple Pay being the most popular mobile wallet. Moreover, merchants consider the mobile option more and more, with 10 out of 100 accepting contactless payments.

"For payments providers, omnichannel has become a point of survival in acquiring today and value-added apps and services are needed to provide next-generation acquiring services" Mrdjan Uzelac, Director Business Development, AEVI

At the same time, OP Financial Group states that mobile is no more needed, and biometrics is the next big enabler in changing the way we pay. Furthermore, the POS-terminal era is ending, and now, the tablet is the innovative and appropriate device for accepting digital payments.

In all this discussion around payment methods preferences, one has the tendency to believe that the customer journey stops at the checkout. It goes without saying that optimizing the checkout page is crucial in today's shopping environment, however, a Valitor report suggests that retailers should look beyond that. Dr. Christine Bailey provided a sneak peek of their upcoming APEX (After Payment Emotional Experience), where customers' feedback after making a purchase is depicted. As a key takeaway, the return process is a hassle, being in several cases time-consuming and costly. According to the report statistics, 50% of consumers say 'no free returns' is the most annoying issue, while 60% won't shop there again. The report might be good guidance for customer retention.

Closing remarks

Cashless, contactless, frictionless - what all these have in common? The same outcome: more convenience. The industry players will increasingly invest in new technologies, to help merchants in delivering the great customer experience that everybody is talking about. Payment service providers will definitely welcome the arrival of SmartPOS, and they will further look into simplifying the payment processing. Overall, the payments industry will still increase its ambition in providing security and convenience, but I believe that this year the focus will be on personalizing digital payments, a customer-centric strategy which is now key given the rise of the ecommerce sales.

We have witnessed some major mergers and acquisitions in 2018, and certainly, we will witness more of these. Big companies see the great opportunity of development via an acquisition, this move being a good way of upgrading their capabilities. What's more, the ecosystem haas started to see the benefits of collaboration, leaving the competition aside.

As for the impact of SCA… let's just all admit that we don't know what will happen next, but with all the technology in place, one will find a way to tackle any challenge that might emerge.

Author: Anda Kania
Source: The Paypers

> "MPE is definitely the place to be for everyone in the merchant and payment business. Filip Rasovsky and his team did an exceptional job on organizing the whole event. Great choice of speakers who provide insights in the payment industry, unique networking opportunities, very interesting side sessions and last but not least great catering."
> Bartosz Skwarczek, G2A.COM

Conference Summary my MPE delegate

Andréa Toucinho, Head of Studies, Prospective and Training, **PARTELYA CONSULTING**

in French langaugue

A Berlin, professionnels des paiements et du retail européens mobilisés sur la construction d'un marché unifié

Réunis à Berlin du 19 au 21 février 2019 à l'occasion du traditionnel salon Merchant Payments Ecosystem (MPE), les professionnels européens des paiements basés en Allemagne mais aussi venus du Royaume-Uni, des Pays-Bas, de Pologne, ou encore de Suisse, d'Italie et de France ont débattu sur les principaux enjeux liés au commerce de demain. Au programme : open banking, acquiring, réglementation, ou encore bitcoin et cryptoactifs.

Comment structurer un marché des paiements européen unifié dans un contexte de fragmentation des usages ? C'est l'une des interrogations qui pourrait constituer le fil conducteur de la série de conférences et meetings s'étant déroulés du 19 au 21 février à Berlin à l'occasion du salon MPE. Basées sur des thématiques distinctes, les sessions ont ainsi toutes eu pour point commun de mettre en avant la pluralité des modèles européens malgré un contexte institutionnel propice à l'harmonisation.

Sécurité : l'importance des standards globaux

Thème phare de cette édition 2019 : la réglementation, et particulièrement les apports de la deuxième Directive sur les Services de Paiement (DSP2) sur les volets sécurité et open banking, avec une mise en avant de l'importance de la création de standards globaux pour assurer « la sécurité d'un marché des paiements européen unifié ». Plus spécifiquement, sur le sujet sécuritaire, au-delà de l'analyse juridique et technologique de l'authentification forte, l'intelligence artificielle (IA) est ressortie des débats à maintes reprises comme innovation à fort potentiel pour assurer une meilleure gestion des risques et une diminution de la fraude. De même pour la biométrie qui permet en plus au consommateur de « reprendre le contrôle » sur l'acte d'achat, avec pour principaux enjeux la garantie de la transaction de bout en bout, bien entendu, mais également une meilleure gestion du risque de réputation, toujours plus détonant dans le marché notamment depuis l'éclosion des débats liés à la protection des données personnelles.

Open banking : la Banque « acteur pivot » de la nouvelle économie

Autre pierre angulaire des débats, l'open banking, perçu comme une source d'opportunités et une évolution naturelle permettant une refonte des modèles et de l'échiquier. Loin d'être mise de côté, la Banque, en tant qu'institution phare, apparaît dans ce contexte comme « l'acteur pivot » de la nouvelle économie. Situation qui suppose néanmoins une évolution plus prononcée vers une logique de co-construction et la création de nouveaux services étroitement liés à la valorisation de la data, au digital et à l'instantanéité, axes phares du nouveau paradigme des paiements. Support par excellence de la société moderne, le paiement mobile devrait peu à peu émerger et trouver tout son sens entre les mains des consommateurs grâce à ce triptyque.

Une situation qui ne remettra cependant pas en cause le marché de la carte, avec une cartographie et des usages adaptés aux différents pays et une activité acquiring qui évoluera de plus en plus vers une logique de « co-construction » entre tous les acteurs – notamment les retailers -, position idéale pour parvenir à une sublimation des stratégies liées à la data et la fidélité dans le contexte de la nouvelle économie, et essentielle si nous prenons en compte les spécificités de certaines régions à l'image de l'Europe centrale et orientale, fragmentées en termes de monnaies, de langues, et de modèles.

Non exclus du débat malgré une vision encore abstraite, bitcoin et cryptoactifs se sont invités dans de nombreuses discussions tournées vers l'analyse prospective de la globalisation du marché des paiements, avec pour illustration phare le Venezuela, célèbre pour son appétence pour le bitcoin. De quoi donner un aperçu de l'évolution des débats à moyen terme.

Author: Andréa Toucinho, Head of Studies, Prospective and Training, PARTELYA CONSULTING

The Balancing Act Between **Strengthening Cybersecurity And Reducing Customer Friction**

Losses from payment fraud amount to $4.19 trillion each year, a sum equal to the combined GDP of the UK and Italy. This is according to Crowe Clark Whitehill, a UK-based audit, tax and advisory firm.

In an effort to protect themselves, companies are therefore often tempted to burden their customers with additional security measures. However, while the fear of payment fraud is certainly justified, innovative technologies can help organizations mitigate this threat without alienating customers—leading to secure business growth.

Ongoing revolution in the payment ecosystem

In today's digital economy, the process of paying for goods and services has never been easier, and consumers clearly approve.

Amazon's 1-Click service became the gold standard for quick and easy online checkout. Select your item or gift and, with a single click, the order is paid for and on its way. For its mobile shoppers, Amazon has even updated the 1-Click service with a new swipe feature.

Another example is Apple Pay: Estimates from Loup Ventures, a venture capital firm, suggest there have been 127 million Apple Pay users worldwide in 2017. Add in payment options from Samsung and Android, and the total number of customers using this "tap and go" method of payment is expected to exceed 500 million by 2021.

And then there is Uber, which has perfected the ultimate in payment ease. After your Uber ride gets you to your destination, you simply exit the vehicle and get on with your day. No wallet. No credit card. No cash.

By storing their customers' credit card or other payment information in their system, these businesses have eliminated crucial steps in the payment process, giving customers a more streamlined and enjoyable experience.

Google is trying to make it even easier for its user base. Google Pay allows users to tap into any payment card they have on file, rather than those they have specifically saved to Android Pay.

So, why are some digital businesses hesitant to adopting card-not-present payment processes?

Two of the most common responses to that question are "How do you ensure online security without degrading the customer experience?" and "How do you choose between customer experience and security?"

Alas, this antiquated notion of having to sacrifice the customer experience to secure online transactions is still out there. After all, businesses are trying to protect themselves from what seems like an endless wave of cyberattacks. In the second quarter of 2018 alone, for example, the ThreatMetrix Digital Identity Network detected 151 million attacks.

How to tackle authentication challenges

Custom-fit for the digital economy, digital identity verification offers businesses an opportunity to be one step ahead of cybercriminals.

Digital identity solutions instantly recognise legitimate users and block out threats by using shared global intelligence. This is combined with advanced behavioural analytics and a clear-box approach to machine learning to connect the dots between the continuously changing associations among people, their devices, locations, credentials and online behaviours in real time.

Technologies such as ThreatMetrix Smart Authentication combine this dynamic intelligence with a strong customer authentication approach. That approach includes mobile app security, device binding, multifactor authentication secure notification and biometrics – all designed to reduce false positives and friction throughout the customer journey.

Once trusted identities have been established, companies can confidently expand their online offerings into new geographies and increase market share. In other words, they are able to securely grow their business.

That doesn't sound like something businesses should be afraid of, does it? In fact, it is something they can celebrate.

Author: Seyfi Günay, Senior Director of Financial Crime and Compliance, EMEA, LexisNexis Risk Solutions

Regional payment specifics: **Russia**

Payment landscape in Russia increasingly moves to digital, and the PSPs face the challenging task of providing 146 million Russian customers with a full variety of different payment scenarios as technologically advanced and user-friendly as possible. Considering the growing demand for foreign companies on Russian market, Yandex.Money, the largest online payment service in Russia, shares its thorough knowledge about payment practices of wide Russian audience involved in buying locally and globally.

Payment habits of Russians

Russia has experienced a cashless payment boom over the past decade. As Mediascope reports, bank cards (88.9%), online banking (87.2%), and e-wallets (71%) were the solid payment preferences of Russian customers in 2018. E-wallet turned out to become a Russian payment phenomenon similar to WeChat Pay and Alipay in China and PayPal in the US. Currently, 48.5% of Russians use Yandex.Money e-wallet, which is 1.5 times more than in 2017. We have already introduced a number of features unique for local market, including in-app analytics in cooperation with American fintech Moven, real-time cashback, platform with frequently updated offers, tokenization of cards, payments with QR-codes. Retail giants like AliExpress, Calzedonia, iHerb, and ASOS adapted to this peculiarity by adding e-wallets to available payments methods.

In 2018, Russia witnessed a considerable rise of contactless payments: 36.3% of Russians pay contactless. As

VISA reported last August, 4 of 10 transactions in Russia are contactless. NFC-reader is a common feature of POS-terminals and ATMs, and the drivers of this trend were banks and PSPs, whereas Yandex.Money was one of the pioneers behind introducing these options to the market.

Fintech landscape at a glance

Fintech in Russia is flourishing, and payment infrastructure is one less thing to worry about while starting or localizing a business here. Last year, Yandex.Checkout and Sberbank introduced a revolutionary product on the B2B payments market: fast and seamless online payments for companies based on B2C payment experience. Right now, most B2B payments in Russia are offline and take about three days, whereas this new solution enables companies make immediate transfers to their suppliers and helps sellers accelerate warehouse turnover.

Innovation and the faster transfer of enriched and consolidated payment data bring the higher risk of fraud, and fintech companies are leveraging AI against scam and fraudulent behavior. This is why we have created an antifraud system, FraudDetector, guarding every transaction of 46 million Yandex.Money's users and 90,000 Yandex.Checkout's partners around the globe. Security shouldn't be disregarded in financial and payments ecosystems in our digital age.

Future of Russia's eCommerce

Recently Morgan Stanley bank experts predicted a nearly threefold growth in Russian e-commerce market for physical goods over the next five years: it will grow to $31 billion by 2020 and probably reach $52 billion by 2023. In the coming years, investments in the Russian market could reach $1 billion, according to Morgan Stanley, and we, in turn, will see an increasing interest of foreign companies in local market.

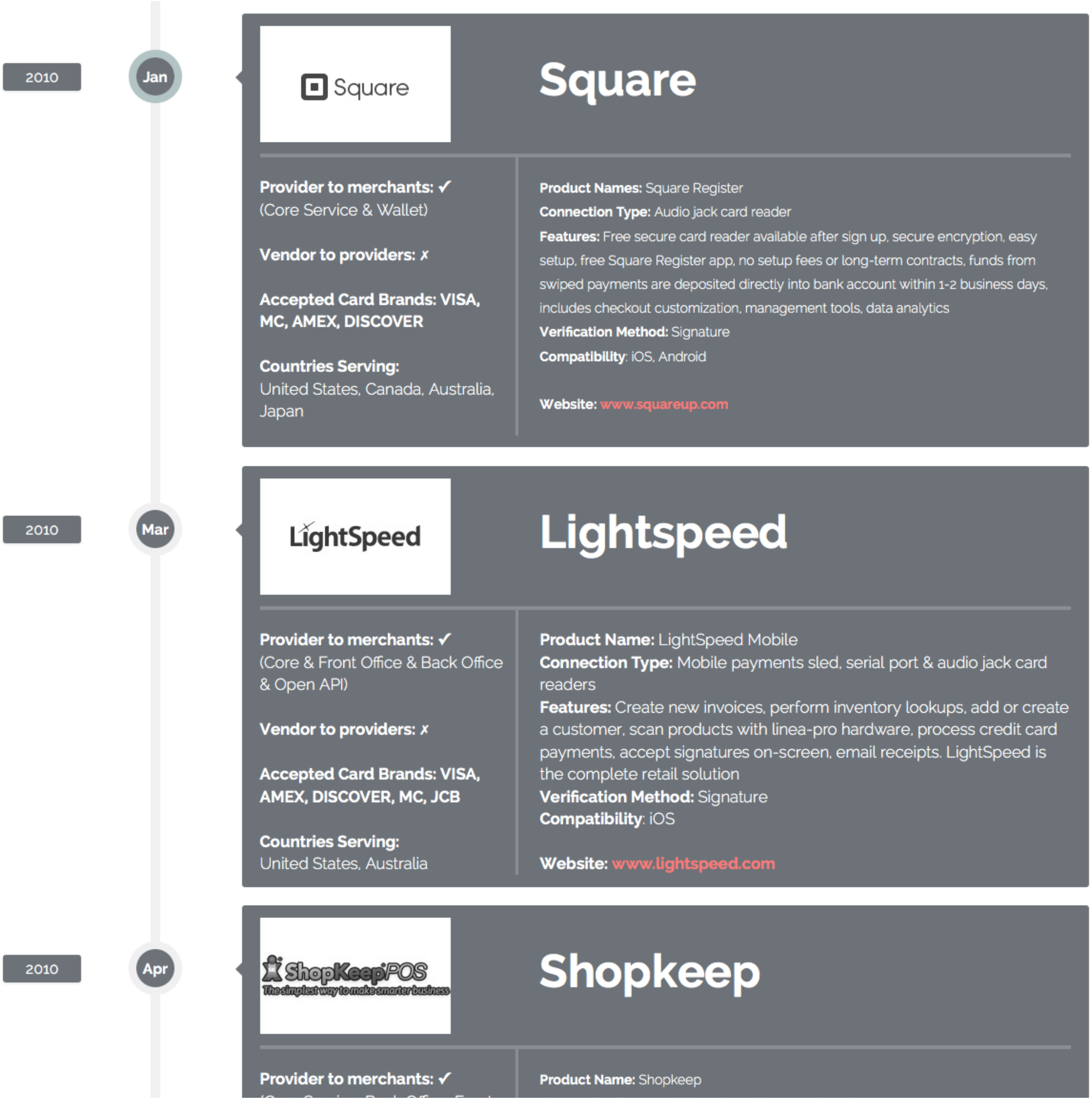
Social commerce is another "new black" in Russia. According to Data Insight and Yandex.Checkout, sales of goods and services via social networks, in instant messengers, on classified ad platforms, and via other P2P platforms, are estimated at approximately $8.98bn and 394 million transactions. Yandex.Checkout, named best PSP by MPE 2019 judges, was the first in Russia to enable online stores to accept payments via messengers, e.g. Telegram Bots or Viber. I say, staying one step ahead is the key to success.

Author: Ivan Glazachev, CEO at Yandex.Money

Global Map of mPOS Providers

The most comprehensive industry overview of mPOS providers. The interactive map monitors the increasing complexity of mPOS ecosystem listing players coming in from different sectors around the Globe.

www.merchantpaymentsecosystem.com



2010 Jan

Square

Provider to merchants: ✓
(Core Service & Wallet)

Vendor to providers: ✗

Accepted Card Brands: VISA, MC, AMEX, DISCOVER

Countries Serving:
United States, Canada, Australia, Japan

Product Names: Square Register
Connection Type: Audio jack card reader
Features: Free secure card reader available after sign up, secure encryption, easy setup, free Square Register app, no setup fees or long-term contracts, funds from swiped payments are deposited directly into bank account within 1-2 business days, includes checkout customization, management tools, data analytics
Verification Method: Signature
Compatibility: iOS, Android

Website: www.squareup.com

2010 Mar

Lightspeed

Provider to merchants: ✓
(Core & Front Office & Back Office & Open API)

Vendor to providers: ✗

Accepted Card Brands: VISA, AMEX, DISCOVER, MC, JCB

Countries Serving:
United States, Australia

Product Name: LightSpeed Mobile
Connection Type: Mobile payments sled, serial port & audio jack card readers
Features: Create new invoices, perform inventory lookups, add or create a customer, scan products with linea-pro hardware, process credit card payments, accept signatures on-screen, email receipts. LightSpeed is the complete retail solution
Verification Method: Signature
Compatibility: iOS

Website: www.lightspeed.com

2010 Apr

Shopkeep

Provider to merchants: ✓

Product Name: Shopkeep