



# POSITIVITY magazine

THE OFFICIAL MAGAZINE OF MERCHANT PAYMENTS ECOSYSTEM • ISSUE 82 / DECEMBER 2019



## FUTURE OF MERCHANT PAYMENTS

Do we  
need oversight  
coordination?

*on page 6*



Airbnb  
to process  
EU payments

*on page 12*



The California  
Consumer  
Privacy Act

*on page 19*





MERCHANT  
PAYMENTS  
ECOSYSTEM

18-20 Feb 2020

BERLIN

## ■ Europe's Largest Merchant Payments Conference



**1250+**  
ATTENDEES



**350+**  
C-LEVEL EXECS



**40+**  
COUNTRIES



**75+**  
SPONSORS  
& EXHIBITORS



**140+**  
SPEAKERS

MPE connects Leaders, Influencers & Innovators from the **ENTIRE PAYMENT ECOSYSTEM**.

MPE is the only inclusive European discussion platform for merchants, acquirers, PSPs, and Point of Sale vendors, established companies as well as start-ups, fintech, regtech and paytech and everyone in between.

**MPE 2020 is the European event with the**

**BIGGEST MERCHANT PRESENCE**

Expect **300+ merchants** representing big brands & various merchant categories

visit MPE website:

[www.merchantpaymentsecosystem.com](http://www.merchantpaymentsecosystem.com)



# MPE 2020 KEY TOPICS

The NEW powers of payment acceptance

The status quo of PSD2, SCA & GDPR

All-in-one payment platforms\*

Transformation, or the end of global acquiring? Strategies & business models

Open banking & API's

RETAIL 2030: The What, Why, and How of retail's future

AI, Machine learning & IoT

Blockchain, cryptocurrencies & payments

Going cashless in the new era of commerce

Merger & Acquisition Frenzy

Fin-tech startups re-building payments

Challengers vs Incumbents - Innovation POV

People for payments - Leadership & Talent\*

New entities on the horizon of PSD2

Changing face of customer shopping journey

Marketplaces & social media commerce

B2B payments

Payment innovation in different merchant verticals\*

Spotlight on Asia

TRUST, Security & fraud prevention

Retail POS innovations and trends

Digital Identity 2.0

Tech giants: The growth of Superplatforms

Payments compliance 2020

Industry-specific ways to pay: Cards vs. APMs



# ADVISORY BOARD



**David Birch**

Director of Innovation  
Consult Hyperion



**Silvia Mensdorff-Pouilly**

General Manager  
European Payments  
Intermediaries  
ACI Worldwide



**Paul Adams**

International  
Payments Director  
Barclaycard



**Christine Bailey**

CMO  
Valitor



**Ron Kalifa**

Vice Chairman  
Worldpay



**Martha Mghendi-Fisher**

Founder  
EWPN



**Michael O'Loughlin**

Vice President, Global  
Solutions  
Token



**Nathan Jackson**

Managing Director  
Presentify



**Ghela Boskovich**

Head of Fintech &  
Regtech Partnerships  
Rainmaking  
Innovation



**Gijsbert Van der Poel**

Head of Card  
Acquiring  
Raiffeisen Bank  
International AG



**Oksana Korobkina**

CCO  
Yandex.Money



**Boris Griesinger**

Head of Payment &  
Finance Projects  
HUGO BOSS



**Debbie Crawford**

Vice President,  
Acquirer Management  
Europe  
Mastercard



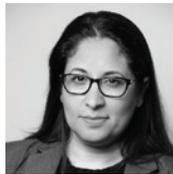
**Steve Cook**

Specialist Biometrics  
& Fintech Consultant  
Biometrics for  
eCommerce



**Amit Kurseja**

Head - External  
Payments  
Amazon Pay India



**Dikla Sharabi**

Director of Shipping &  
Payments  
Tenengroup Ltd.



**Carl Churchill**

Owner & Managing  
Director  
NetPay Solutions  
Group



**Peter Kovacs**

Sr. Product Manager  
The New York Times



**David Parker**

CEO  
Polymath Consulting



**Melisande Mual**

Managing Director  
The Paypers



**Zachary Powers**

Director of Payments  
Strategy  
FareHarbor &  
Booking.com



**Carlos Gutierrez  
Arguello**

Open Innovation and  
Partnership Director  
Demtech International



**Faheem Bakshi**

Head of Payments  
Kinguin



**Christian Bucheli**

Strategy and M&A  
BS PAYONE



**Ron van Wezel**

Senior analyst  
Aite Group



**Paul Rodgers**

Chairman  
Vendorcom

# MPE 2020 Key topics

What's next for merchant payments' ecosystem in 2020?  
MPE 2020 speakers provided the answers

## Future of merchant payments, new business models and technologies supporting commerce and payments

The way people pay is changing rapidly, thanks to technological innovation and digitalization. Society is becoming increasingly cashless as more consumers choose to rely on cards, as well as alternative payment methods. At present, less than 50% of all payments in the UK are made with cash, and if this trend continues then by 2026 it is predicted that this figure will drop to 21%. In 2019, Mobile technology is changing the way we pay, with m-Commerce constituting 56% of all e-commerce sales, with an estimated \$3.6trn in m-Commerce sales by 2021.

The changing payments landscape challenges everyone. For merchants, payments are no longer just a cost of doing business but can drive growth, if approached holistically by them. Currently, only 20% of merchants have a mobile payments app and only 40% have a mobile-centric payments website.

On top of that, there is a myriad of new technologies like Artificial Intelligence (AI), Machine Learning (ML), biometrics, etc. impacting commerce & payments. The Internet of Things creates a seamless web of touchpoints, through integrated apps, smart devices, and integrated payments, making electronic payments even more convenient.

Instant & Mobile payments are poised to finally have its day thanks to APIs and open banking. New channels appear seemingly overnight. In 2020, "Social Commerce" and "Voice Commerce" are looking likely to become part of our everyday life. There will be more "Value Added Services" including loyalty and coupon offers that are seamlessly integrated into payment transactions. In this context, delivering a unified mobile payment experience is the new challenge in the battle for the consumer.

Omnichannel integration can be an overwhelming task for merchants. Over 50% of Retailers are focused on creating a

consistent brand experience across channels. On the way to optimizing payments for omnichannel commerce, there are many questions for both payment providers and merchants.

At MPE2020, the Biggest European conference on merchant payments (Berlin, Feb 18-20), over 140 inspiring speakers will provide unique insights on what payment providers are doing to help merchants to achieve frictionless shopping experience. MPE team asked few of Merchant payment industry leaders and MPE speakers, how payment providers are changing business models, adapting their legacy systems and how to use payment data to help merchants increase sales?

### **How should the payment companies change their business models to adapt to the new era of instant & mobile-driven payments in 2020-?**

According to Jeremy Nicholds, CEO of Judopay who will speak about the psychology of mobile payments at MPE2020: „If you're looking to build a case for technology investment, explore your business growth goals and how this new payment technology can support these plans.“

### **The important question for incumbent players is whether to substitute or adapt their legacy systems to cope with the new market standards & technologies?**

Ruca Sousa Marques, CEO of Switch, who will cover the Interoperability in the Payments Industry in his speech at MPE2020 said: „There's value in existing legacy systems—they're still performing valuable actions! What's needed though, is to decouple traditional monolithic architectures into microservices setups, ones that allow for interoperability between internal/external systems, thus accelerating integrations with 3rd party vendors for quicker go-to-

market strategies. For this matter, a middleware is necessary to orchestrate communications through standardized data structures, avoiding any updates in back-office systems every time a new application is connected. In his presentation, he'll propose a new model for adapting legacy infrastructures to new market standards (e.g. Mobile, PSD2, 3DS v2.0, APMs, Omnichannel), capitalizing on existent systems and preparing incumbent companies for the challenges ahead".

**If UX and Data is the new oil of Payments, AI and ML will be critical to the innovation of payments and related shopping experience and fighting the fraud. The important question is how to use data effectively to build a strong and secure customer engagement strategy?**

Martin Sweeney, CEO at Ravelin advises: Work with a partner who has the resources and expertise to help you. For large enterprises, this means working closely with your fraud partner rather than relying on a payment provider to take responsibility for your fraud. It's likely you'll need to work with more than one payment provider, which makes it more effective to do the risk analysis and manage your fraud pro-

tection yourself. You have the most data on your customers, transactions and the fraud you're facing. This puts you in the best position to derive the insights and results you need. I also recommend sharing knowledge when it's appropriate. Since we founded Ravelin, we've seen a huge increase in collaboration between merchants, which is fantastic. We wholeheartedly support this and try to contribute through participating in industry events like MPE, hosting our own events and creating merchant-led content.

You can read the entire interviews in the POSitivity magazine, section Interviews.

Future of merchant payments, new business models and technologies supporting commerce and payments are among the key topics to be discussed at the MPE 2020, Europe's Largest Merchant Payment Acceptance Conference in Berlin, February 18-20.

Request the Agenda & register at [www.merchantpayment-secosystem.com](http://www.merchantpayment-secosystem.com)

# European Cards industry in 2020 and beyond.

## Do we need oversight coordination?

PSD2 SCA has been one of the most discussed topics for merchant payment professionals before and after its implementation deadline, on September 14, 2019. What are the lessons learned from the PSD2 SCA implementation project so far?

### What has happened in 2019?

- January – September 14: Many industry players have advocated before September 14 for a pan-European migration plan that is consistent, harmonized and effective across all member states.
- June 21: In view of the complexity of the enforcement, on June 21, 2019, the European Banking Authority (EBA) granted National Authorities (NAs) the possibility to postpone the 14th September deadline in order to allow the implementation of new authentication tools by all customers, with exclusive reference to the

online card payments.

- June – October: Several NAs announced different migration plans, so there is a risk of differences in implementation. If that happens, it will be difficult, expensive and time-consuming for payment providers and merchants to prepare their solutions.
- October 16: the European Banking Authority (EBA) published another Opinion on the updated Payment Services Directive (PSD2) and in particular its provisions on Strong Customer Authentication (SCA). The Opinion recommends that National authorities (NAs) grant issuers and acquirers (PSPs) until 31 December 2020 (i.e. a 15-month extension) to comply with the SCA requirements for remote card-based payments, subject to compliance with certain intermediary milestones.

MPE 2020 conference team interviewed 14 different mer-

merchant payments industry professionals before and after September 14 and October 16 to bring the feedback of the merchant payments ecosystem. MPE summarised their feedback and here are the KEY LESSONS LEARNED from the PSD2 SCA implementation project according to various industry professionals:

**.... Coordinated approach is needed....**

**.... The installation of a program management office needs to happen...**

**.... there is a need to reorganize oversight of this industry.**

**... a lack of consistent communication with consumers and a general failure to prepare merchants for the impact of SCA in eCommerce...**

Alan Moss, Head of Fintech & Payments BluSpecs & MPE 2020 conference moderator also provided his feedback on: What now needs to happen to make the transition a success after October 16?

“The 14th of September deadline certainly provided a sharp focus on SCA implementation for merchants and service providers alike, with a real threat of business disruption as the cliff-edge drew near. In the end, the deadline came and went without any significant problems being reported in eCommerce traffic.

Given the apparent unwillingness of the EBA to recognize the potential chaos that could ensue from a literal interpretation of its deadline, local banking regulators (or NCAs), had begun to take matters into their own hands. A series of national pronouncements followed, which seemed to vary from strict adherence to the original deadline in the case of Denmark, to a 3-year migration period set out by France.

Finally, on the 16th of October, the EBA published its own opinion, effectively granting a 15-month extension, and setting out a very detailed implementation plan to be followed by issuers and acquirers/PSPs, and enforced by local regulators. This certainly adds to the confusion, given that many regulators had already communicated plans which are now at variance with the opinion of the EBA. As a result, there is still the possibility that SCA implementation is implemented according to different schedules and with varying degrees of policing in the various European nations.

On top of this, there remain some doubts about the

ability of merchants to have fully compliant and working solutions in place by the revised EBA deadline: SCA is dependent on the adoption of the new 3DS V2.2 specification, which will not be mandatory for issuers until September 2020, according to at least one major scheme. Testing will then be in progress right through to March 2021, so in my opinion, there's little chance that all merchants will be fully SCA enabled and PSD2 compliant by the end of December 2020.”

You can read full interviews with 14 different industry professionals in the report “SCA transition plans across Europe & industry perspectives”. To download the report please visit: <https://www.merchantpaymentsecosystem.com/intelligence-mpe/reports/SCA-transition-plans-across-Europe-and-industry-perspectives>

Join MPE 2020 conference, Berlin, February 18-20 to learn from different industry stakeholders about

- what needs to happen to make the SCA transition a success after October 16? and
- if there is a need for a coordinated oversight of the card & merchant payments industry in Europe.

MPE 2020 is Europe's Largest Merchant Payments conference.

1250+ attendees, including 300+ merchants, 400+ acquiring banks & PSPs from 40+ countries come to network and be inspired by 140+ TOP industry speakers, 75+ solution providers.

Register NOW, with special winter rates valid through December 31:

10% off on passes = 2250 EUR, (Regular price: 2500 EUR). <https://www.merchantpaymentsecosystem.com>



## SCA transition plans across Europe & industry perspectives

Prepared by:  
Natalia Ivanis,  
Head of Marketing & Media partnership  
[natalia.ivanis@merchantpaymentsecosystem.com](mailto:natalia.ivanis@merchantpaymentsecosystem.com)



## Selection of Merchant Payments' Industry Mergers & Acquisitions Q3 & Q4/2019



### October 2019 - Mastercard buys Session M for merchant loyalty and marketing services

SessionM, is a U.S.-based technology company. SessionM's customer engagement and loyalty platform empowers the world's most innovative brands—including retailers, airlines, restaurants and CPG companies—to forge stronger and more profitable consumer relationships. The addition of SessionM will enhance Mastercard's ability to help brands around the world deliver personalized, real-time offers and comprehensive campaign measurement based on robust, data-driven insights. Terms of the agreement were not disclosed and the transaction is anticipated to close in the fourth quarter.

Source: [Mastercard](#)



### November 2019 - Elavon Acquires Sage Pay, Expanding Its Presence and Services for Customers in the UK, Ireland

Elavon, global merchant acquirer and subsidiary of U.S. Bancorp (NYSE: USB), has agreed to acquire Sage Pay, a well-known and established payments gateway business in the United Kingdom and Ireland. Sage Pay is a division of The Sage Group plc (SGE), a FTSE-listed market leader in cloud business management solutions. The acquisition is part of Elavon's strategy to help its business customers grow as the global economy becomes more digital, and as businesses look to streamline their operations with software that includes payments capabilities. Elavon is currently the fourth-largest merchant acquirer in Europe with an integrated international processing platform that allows them to do business in many countries and currencies. This acquisition extends Elavon's market share in the UK and Ireland, particularly for small and medium-sized enterprises where Sage Pay is a highly-trusted payments gateway with a loyal customer base.

Source: [Business Wire](#)



### October 2019 - Payroc Merges with Payscape, NXGEN and BluePay Canada

Payroc LLC, a leading merchant acquirer and payment processor, is excited to announce it has entered into a definitive agreement to merge with Payscape, NXGEN International, and BluePay Canada. The transaction creates a full-service global merchant acquiring and payment facilitator powerhouse operating in 46 countries, while serving more than 55,000 merchants processing \$23 billion in annual bankcard volume. Advancing into the top ranks of non-bank merchant acquirers, the combined enterprise, with its additional capabilities, will carry a new and enhanced Payroc brand. The new Payroc is poised to drive rapid expansion and growth through sales, marketing and forward-facing technology integrated with proprietary U.S. and international front-end and back-end processing platforms.

The merger was sponsored by Parthenon Capital, a growth-oriented private equity firm that focuses on building franchise assets in the financial services and health care sectors. Payroc, the new combined enterprise, will maintain significant operational presence in Chicagoland, Atlanta, Toronto, Whitefish, Montana and Salt Lake City. The company is a high-growth American, Canadian and international merchant acquirer, processor and payment facilitator powerhouse operating in 46 countries, processing \$23 billion in annual charge volume for more than 55,000 merchants.

Source: [Business Wire](#)

## Selection of Merchant Payments' Industry News Q4/2019

### Toscafund invests EUR25m in Lemon Way

Pan-European payment processor, Lemon Way has secured a EUR25 million investment from London-based specialist financial services investor, Toscafund Asset Management (Toscafund). The transaction is Toscafund's first private equity investment in France.

Lemon Way is a Paris-based regulated payment institution focusing on marketplaces, crowdfunding platforms and e-commerce websites that require payment process-

ing, wallet management and third-party services in a KYC/AML-regulated framework. It currently manages over seven million payment accounts. Lemon Way offers an all-in-one solution of modular and proprietary API-based services ranging from on-boarding to cash pay-out flows.

Source: [Private Equity Wire](#)

### Visa makes strategic investment in LISNR, a start-up that wants to rival technology used by Apple Pay

LISNR, a start-up that is using ultrasound technology as a mobile authentication and mobile payments solution, has received a strategic investment from Visa, and the financial services giant and LISNR will now begin to deploy the technology in merchant mobile wallets and with the everyday mobile transactions consumers are making.

The Cincinnati-based start-up announced on Tuesday that Visa took part in a recently closed Series C venture capital fundraising and is now working with LISNR on commercial beta-testing of its mobile payments technology with retail merchants. This investment comes at a time when large tech companies, like Apple with Apple Pay, are growing in the mobile payment market using near field communication technology (NFC).

Founded in 2012, LISNR uses inaudible ultrasound technology to transfer authentication and payment data through sound waves between devices.

"The way in which people are paying for things will

dramatically change," said Rodney Williams, LISNR co-founder and chief commercial officer in an interview on Monday with CNBC. "This is a major validation and also a major market signal for the world of payments," he said of Visa, which he described as the "largest mobile wallet company in the world."

Visa did not respond to a request for comment by press time.

In late 2018, LISNR announced a deal with Equinox Payments, a payments technology company owned by Brookfield Asset Management, which was the first to test its ultrasound technology for payments through Equinox point-of-sales systems. Williams told CNBC that deal was focused on private-label cards, not "open loop payments," which link a credit or debit card directly to a device, a focus for consumer technology companies.

Visa and LISNR do have a history together: The start-up was one of three young companies chosen by Visa back in 2015 to take part in a design challenge focused on



future commerce and payments technology.

Williams previously has said Visa's Everywhere Initiative opened up the possibility of using sound to support payments and other financial services use cases. The company has worked with Visa to validate the concept in recent years, though the two never had a commercial relationship until now.

LISNR's plans for its payments growth include enabling merchants and payment providers to universally accept mobile payment data across scan-and-go retail, store pickups, pay zones, point-of-sale, home-based e-commerce, and even voice-enabled purchases.

"With this investment and commercial relationship, Visa further validates LISNR's push into retail as LISNR brings to market an improved mobile payment product across a wide range of use cases," the start-up said in a Tuesday release.

LISNR is also planning to work with Visa in additional payment use cases in mobility, transportation and ticketing.

LISNR vs. current Apple Pay tech and others

Williams said one advantage of the LISNR system is that it is safer and more secure than other contactless technology, like QR codes, which can be easily replicated. Additionally, it does not require expensive hardware like the near-field communication technology used by Apple's Apple Pay. Samsung Pay and Google Pay also use NFC technology.

"Our true advantage over NFC is that LISNR is all software and not restrictive to the OEM, as only the OEM provider can use NFC vs. any merchant having the ability to use LISNR in their mobile wallet," Williams said.

Arieh Levi, senior analyst at research and consulting firm CB Insights, said that while NFC technology is more secure than QR codes, it is much more expensive to implement.

"We will remove the open-the-app-and-scan (QR) or the tap (NFC) in a secure way that will speed up the transaction time and allow consumers to get in and get out faster than ever before," Williams said.

Mobile pay in the U.S. lags the rest of the world, and one reason is hardware cost. To use options like Apple Pay, Google Pay and Samsung Pay, merchants such as coffee shops and retail stores need the proper hardware. "It's expensive," Peter Gordon, CEO of PRMPayments, recently told CNBC.

U.S. mobile-phone payment transactions made at physical retail locations, typically using NFC technology, are expected to reach near-\$100 billion in 2019, grow 31.8% to \$130.36 billion next year, and by 2021 the total transaction value will reach \$161.41 billion, according to a forecast from eMarketer. Apple Pay is expected to be the leading source of transactions.

Williams said merchant wallets are 62% of total mobile wallet transactions and the biggest players are actual merchants like Starbucks, Walmart, and Target. He said Apple Pay is a competitor to merchant mobile wallets.

In recent years audio has been adopted in a growing number of use cases to connect technology, from Google's Chromecast streaming connections to video game data transfers, and ticketing at events, an area in which LISNR has been a leader, working with Live Nation Entertainment's Ticketmaster.

LISNR's first big deal was with Ticketmaster for mobile authentication at events as a replacement for QR code-based scanning of mobile tickets, but more recently it has pivoted its business model to ramp up mobile payments.

Williams said payments and mobility authentication are the sole focus areas of LISNR today.

LISNR, which ranked No. 41 on the 2019 CNBC Disruptor 50 list, has partnerships with more than 100 other companies in various industries. Its existing investors include Intel, Jump Capital, Mercury Fund, R/GA and private-label credit card company Synchrony Financial.

Williams said payments is the biggest opportunity of all.

“Payments in general has a much bigger market opportunity for disruption than any other vertical. This announcement with Visa is the first of many commercial announcements of financial institutions and merchants

moving forward,” Williams said.

He declined to specify merchants currently in beta-testing through the new Visa commercial relationship.

Source: [CNBC](#)

## CaixaBank, Global Payments and Ingenico Group partner to create an **international innovation programme supporting startups** in the fintech and business sectors

CaixaBank, Global Payments and Ingenico Group join forces to launch an international innovation programme aimed at startups with the objective of contributing to promoting the creation of new products and services for the business and fintech sectors. The project, Zone2boost, will be established as a new company owned by CaixaBank (40%), Global Payments (40%) and Ingenico (20%) and will rely on IESE as collaborating entity.

The programme was presented today in Barcelona at a press conference participated by Juan Antonio Alcaraz, CaixaBank’s Chief Business Officer; Jeff Sloan, Global Payments’ CEO; and Mark Antipof, Ingenico’s Global Head of Sales and Marketing.

Zone2boost’s mission is to identify innovative technology initiatives for businesses and financial services and support their growth. The selected startups will obtain funding and access to a physical space to develop their projects, as well as work in collaboration with other innovative companies and a team of expert mentors that will provide customized training and advice. Additionally, DayOne, CaixaBank’s division providing specialized services to startup businesses, will offer tailored financing.

As a part of collaboration with the project’s partner companies, entrepreneurs participating in this initiative will be given the opportunity to have access to their customers. CaixaBank, Global Payments and Ingenico Group will have preference incorporating a project developed by the startups into each of their commercial offerings.

It is estimated that the support provided to these entrepreneurs will range between six months and two years, throughout which the new companies will evolve from very early stages to a stage that will enable them to access the market.

The programme will be open to studying startups from around the world, although initially it will focus on Barcelona, the city in which the activity will kick off and also where the workspace will be located (Pier02, Barcelona Tech City).

The initiative will be launched in the last quarter of 2019 and will entail an initial investment of five million euros over the next three years. Once the space is fully operational, it is expected to be able to accommodate approximately thirty companies.

The creation of this international innovation programme for startups has led to a new innovation partnership between companies, following the successful creation of the Payment Innovation Hub by CaixaBank, Global Payments, Samsung, Visa and Arval in 2017.

Also located in Barcelona, it is one of the first hubs in the world to be launched by a multisectoral partnership of companies, all of which are leaders in their respective sectors.

Source: [Ingenico](#)

# Airbnb to process EU payments via Luxembourg as Brexit looms



Airbnb will process payments between hosts and guests for the European Union through Luxembourg as of 2020, as the home rental giant prepares for Britain's

departure from the bloc, Luxembourg for Finance said on Wednesday.

Airbnb, which was founded in 2008, set up a hub in Luxembourg at the end of last year and has now been granted a payment institution license, Luxembourg for Finance, a body which promotes the country's financial sector, said. [bit.ly/386iBmf](https://bit.ly/386iBmf)

Payments sector giant PayPal Holdings, Amazon Payments, Rakuten and Alipay have picked Luxembourg as their hub to serve the European Union, Luxembourg for Finance said.

Source: [Reuters](#)

## Twenty European banks working on setting up a pan-European payment system - PEPSI

Twenty European banks are working on setting up a pan-European payment system to bypass Visa, Mastercard and technology companies such as Google and PayPal, confirmed to AFP sources involved in this project.

According to the sources, the Pan European Payment System Initiative (PEPSI) is aimed at managing all forms of cashless transactions.

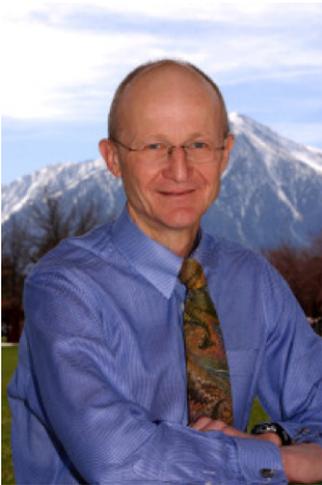
The idea came from the European Central Bank, which has been pushing for a system to allow Europeans transfer money to each other instantly, a French banking source close to the subject said. The ECB was "worried

about the sovereignty of payments and explained that it would appreciate if we looked into the issue," adding that it was chiefly a "political not a technical initiative", said the source.

None of the banking groups contacted by AFP would speak openly about the project. However, according to various sources, only banks from countries in the euro zone (Italy, Germany, France, the Netherlands, Belgium, Portugal, Spain) are involved in the initiative, including a large part of French banks and Deutsche Bank in Germany.

Source: [Paypers](#)

# Faster payments' public option will harm competition



In August the Fed announced it intends to launch a real-time interbank payments service called FedNow. The central bank wants to do good. That's neither sufficient nor its call.

[Rep. Denver Riggleman, R-Va., cautioned the Fed against spending hundreds of millions of dollars to enter the real-time payments market. It'll cost considerably more.](#)

As an individual representative perhaps his tenor is appropriate, but for Congress it's unduly deferential. While Congress has too often abdicated its constitutional prerogative to make law, set policy for and instruct the "independent" and executive agencies, Congress is supposed to be master and the Fed its servant.

At the [Senate Banking Committee's Sept. 25 pro forma hearing on "Facilitating Faster Payments in the U.S."](#) senators, for the most part, were even more deferential than Riggleman.

President of the Kansas City Fed Esther George testified other providers alone couldn't be expected to provide the service "with reasonable effectiveness, scope and equity," there was "a clear public benefit," and the Fed would fully recover its cost "over the long run." When gently pressed on the need for FedNow she insisted rural and community banks could only be well served by the Fed. Hiding behind the skirts of politically sympathetic community banks is a time-honored practice in Washington.

Senators and witnesses extolled competition, and, with big banks' cooperative processor The Clearing House in mind, worried about centralization and concentration

of power. Ranking member Senator Sherrod Brown, D-Ohio, vilified big banks. The ultimate concentration of power in the financial system, however, isn't TCH or dastardly large banks. It's the Fed.

In contrast, Senator John Kennedy, R-La., asked why the Fed should spend taxpayer dollars to compete with the private sector and suggested FedNow advocates "just wanted to expand government."

Former FDIC Chair Sheila Bair contended the payments system is a "public utility" and was keen for the central bank to expand its role. But, where practicable, America has long preferred robust private-sector competition over public utilities exempt from antitrust law. In retail electronic payments, government has never played a significant role. Competing networks like Visa, Mastercard, American Express, PayPal, Discover, Star and NYCE deliver enormous value, relentless innovation and near-ubiquitous access. TCH has been an interbank processor since 1853.

The Fed used its bully pulpit to socialize the value of faster interbank payments and encourage the private sector to enter the market. TCH took the challenge and spent \$1 billion building a real-time-payments system, launched in 2017. A single provider, however, would be a bad outcome. The only thing worse would be no supplier. Indeed the [most compelling rationale for the central bank entering the instant-interbank payments market would be to ensure there wasn't a monopoly.](#) If you define a market narrowly enough you can always conjure a monopoly.

However, in addition to TCH, there are a handful of competing real-time interbank payment systems.

Leveraging their card-delivery systems, marquee networks Mastercard and Visa, and processing behemoths FIS and Fiserv, serve the market. Mastercard and Visa in particular could be more formidable faster-payments competitors. Directly or indirectly they reach virtually every DDA in America. Moreover, Mastercard owns the

U.K.'s faster interbank payments system Vocalink and is selling the service worldwide. Bank cooperative Early Warning Systems' Zelle too provides instant interbank payments. All have ample technical prowess and existing networks. As competitors they would likely enhance their services, ensuring universal access and providing value continuously market to market.

A whiff of competition works wonders. Cryptocurrency phenom Ripple's nascent cross-border payments challenge forced Swift to up its game. Ripple could as well turn its sights to the U.S. market.

Riggleman rightly notes there's a patent conflict of interest in the Fed competing with entities it supervises and regulates. He fails to note that's been an issue for decades with the central bank's ACH and Fedwire operations competing with the private sector. The conflict suggests the paramount financial system regulator

should divest them.

Even if the Fed weren't regulating private-sector real-time systems, it shouldn't compete with them.

The Fed's entry into the market will have a chilling effect on competition and innovation. Nobody will be keen to go toe-to-toe with the financial systems' paramount regulator and central bank with virtually unlimited resources. It will deter and suppress private-sector operators from investing more in real-time payments. That won't be good for banks, or businesses and consumers they serve.

The Fed like most agencies will take all the leash it's given. Congress should bring it to heel.

Author: Eric Grover, principal at Intrepid Ventures

# UK social commerce (selling on social media platforms) is set to double over the next 6 months

## The social commerce opportunity

Almost one in 4 (24%) British businesses already allows customers to make transactions through their social media channels. That's set to double over the next 6 months as mobile shopping extends into social channels. The stronger customer connection that businesses can build on social channels appears to be valuable. Those that already sell on social say that 38% of their sales volume comes via social media.

That's a big number, but it compares with a global average of 45% of sales volume. UK sellers and buyers are clearly playing catch-up on social commerce. And, that means a huge opportunity for UK businesses to get ahead of the game. Currently 8.4m British consumers shop via social media<sup>2</sup>, with Facebook, Instagram and Snapchat being the most popular channels. A fifth of those already purchasing through social do so weekly, with individual social spending averaging £71 monthly.

## Who's buying what on social media?

Social commerce is growing within all age groups but, as you'd expect, it's the younger demographic that's leading the way. Almost one in 4 (24%) Millennials and just over 1 in 5 (22%) Gen Z-ers have purchased or paid using social media in the last 6 months. That compares with 1 in 6 (17%) from Gen X and 1 in 9 (11%) Baby-boomers. Perhaps unsurprisingly, the top categories for social commerce are Clothing & Accessories (15%) and Health & Beauty (10%). Other popular categories include Home & Garden (8%), Books & Magazines (7%), Food & Drink (6%) and physical Toys & Games (6%).

## Security stays top of mind

The Commerce Index also found that security and trust remain a concern for UK online shoppers. They are also the top priorities for UK online businesses. "Ensuring the privacy of customer data" ranked as the top priority for business (at 34%). "Ensuring the security of our IT/technology system" came a close second (33%).

# AT A GLANCE

## Mobile Commerce Strong Preference in UK



CONSUMERS PREFER TO SHOP ON MOBILE DEVICE (VS 71% GLOBAL AVERAGE)



48%

MOBILE SHOPPERS PAY/  
PURCHASE ON MOBILE AT LEAST  
WEEKLY



36%

ONLINE SALES ARE TAKEN BY  
MOBILE DEVICES

## Social Commerce Lags Behind Global Average



PURCHASED VIA SOCIAL MEDIA IN THE PAST 6 MONTHS (VS 30% GLOBAL AVERAGE)



24%

BUSINESS SELL VIA SOCIAL  
MEDIA



AVERAGE MONTHLY SPEND  
BY SOCIAL SHOPPERS

## Cross Border Shopping International Sales Opportunity



ONLINE CONSUMERS SHOP CROSS-BORDER (VS 55% GLOBAL AVERAGE)



17%

BUSINESS SAID 'SELLING TO  
INTERNATIONAL CUSTOMERS HAS  
HELPED OUR BUSINESS GROW'



10%

BUSINESS ACTIVELY TARGET  
INTERNATIONAL BUYERS

©2019 PayPal Inc. The above is a summary of the 2019 Trend Report. Full report available [here](#).

For shoppers, the convenience of using a mobile device wins out with almost three quarters (73%) of consumers using mobile devices for purchases and payments. Nearly half (48%) use their mobile at least weekly for purchases and payments.

Security or trust issues remain a potential barrier, however, cited by nearly two-thirds (64%) of shoppers. That's the highest level of all the 11 markets surveyed. One in 4 (26%) UK shoppers have abandoned a transaction on mobile because of security concerns.

As social commerce grows in popularity, there will be an increasingly a close eye kept on the data collected during the social shopping experience and its potential implications. No surprise then that this is reflected in the Commerce Index research:

- 39% say "I don't trust the process of buying on social media platforms"
- 38% say "I don't want my financial information linked to my social media"
- 37% say "I am worried about safety / security of my personal information on social media."

To capture the social commerce opportunity, businesses will need to pay special attention to these concerns by providing processes and payment methods that are trusted and secure.

### Don't miss the cross-border opportunity

The Commerce Index research also suggests that the UK's online businesses may be missing out on cross-border sales. While 1 in 3 UK businesses have made international sales in the past 6 months, only 10% of businesses say that they actively target international buyers. But global online shoppers increasingly enjoy cross-border shopping. Our research suggests that more than half (55%) of consumers shop across borders on a regular basis.

The top reasons for shopping on international sites are:

- Access to items not available in their home market (50%)
- Better prices (46%)
- To discover new and interesting products (28%).

Add to that the fact that British brands are often highly valued by overseas shoppers and the research suggests a large and untapped opportunity for the UK's online sellers.

In our research, 17% of business respondents said 'selling to international customers has helped our business grow'.

Source: [Paypal](#)

## Privacy in a Cashless Society

As highlighted in the Access to Cash Panel's final report published in March 2019, consumer concerns over privacy are often cited as a reason that people continue to wish to use cash. In the six months since the report was published, various headlines have highlighted an acceleration in the reduction of free to use ATMs, further bank branch closures and an increase in the number of retailers and public bodies no longer accepting cash as a means of payment; all of which is putting pressure on those who wish to continue to use cash. For those concerned about the privacy of data associated with their transactions, this is a worrying trend.

So, are people right to be concerned over the privacy of their data if they have to switch to using cards or other means of payments? At first sight, it is difficult to argue that the answer is "No". When you walk into a shop and pay by cash, you are leaving no digital footprint behind of your association with the transaction. The retailer's point of sale terminal (and any linked stock control system) will know that a specific item of stock has been sold, but it has no information in terms of the purchaser unless such information is voluntarily provided. The moment a payment is made with a card rather than cash, there is a linkage between the sale of that specific item, the initiation of a payment transaction via the merchant's card acquirer (who would normally supply the point of sale terminal), the handling of the transaction via the card Scheme (e.g. Visa or Mastercard), the transaction authorisation via the card issuer and the subsequent payment from the customer's card issuing bank to the merchant's bank. Data is captured at various points in the transaction cycle and will then be retained (often for years) for regulatory and/or accounting requirements.

At this point, it must be highlighted that no details of the underlying purchases at a store are passed to the acquirers, the card schemes, the card issuers or the banks involved in the transaction. The data remitted will need to adhere to the underpinning ISO 8583 (card

messaging standard. This requires that a variety of data components be captured at the point of sale and passed through for processing (such as the merchant (card acceptor) unique ID, merchant name and location, date and time of the transaction and the total amount). However, a four digit Merchant Category Code is also included in Field 18 of the message which could give insight into the transaction. There are many of these.

Some of those used by Mastercard include:

- 5411 Grocery Stores, Supermarkets
- 5813 Bars, Cocktail Lounges, Discotheques, Nightclubs, and Taverns—Drinking Places (Alcoholic Beverages)
- 5814 Fast-food restaurants
- 5912 Drugstores and pharmacies
- 5931 Second Hand Stores, Used Merchandise Stores
- 5933 Pawn Shops
- 5944 Clock, Jewellery, Watch and Silverware Stores
- 7273 Dating services
- 7995 Gambling Transactions
- 9211 Court costs including Alimony and Child Support
- 9222 Fines

In isolation, a transaction provides only limited information. However, over a period of time, the names and business type of the merchants that a consumer uses and the frequency of transactions would likely provide insights into a consumer's lifestyle if this data was to be inappropriately utilised. Concerns on this have been aired in the media from time to time such as the following article from 2011:

<https://www.foxbusiness.com/features/mcc-codes-unveil-consumer-shopping-habits>

Turning to the retailer (where the underlying details of the transaction is known), things then boil down into two camps; those where the store has an agreement

with the customer that their transaction data may be analysed and those that don't. The former is readily highlighted by store loyalty programmes where a customer may receive incentives such as cashback, tailored vouchers or early access to sales or special offers. In exchange, the Terms and Conditions of such loyalty programmes are likely to inform the customer that their data might be analysed for marketing purposes. A hybrid form is also present where the customer may not hold a loyalty account but, at the point of sale, they are asked by the merchant for their zip/postcode and/or address details. This may be explained for an offer to go onto mailing lists or for warranty/guarantee purposes. Again, customer consent permits restricted use of the data at that point.

Any such data held by a company (or others in the payment chain) must be protected in line with local data protection laws. In countries covered by the EU 2018 General Data Protection Regulations, the obligations relating to data controllers, data processors and the associated rights for individuals "to be forgotten" via Subject Erasure Requests extended the earlier data protection obligations that firms had to follow.

However, data breaches can and do occur. In 2013, the US retail firm Target fell victim to Point of Sale malware, which resulted in the theft of data relating to up to 70 million customers. This resulted in Target settling a class action suit from banks and credit unions for \$39.4m.

Turning back to the core question of whether consumers are right to be concerned over the privacy around non-cash transactions it is easy to see from the examples above how such concerns can arise. For these to be allayed so that these consumers will switch away from cash, more concerted effort and information will likely be needed from retail groups and payment entities as to how consumer data is used, how it is protected, how long it is kept for and the rights of consumers to request that it be deleted.

Author: Phil Kenworthy, Director, Payment Systems Consultancy Ltd

Source: [Payment Systems Consultancy](#)

1 Mastercard quick reference booklet – Merchant Edition (Nov 2018)  
<https://www.mastercard.us/content/dam/mccom/en-us/documents/rules/quick-reference-booklet-merchant-edition.pdf>

## 3 ways big tech are about to disrupt financial services in Europe

Europe has so far been largely protected from the big tech march into financial services. Penetrating each market has been a challenge due to differences in language, tech adoption and regulations. But open banking is unifying the financial landscape across the continent, making it easier for tech giants to get a foot in. Now the big questions are: what will happen when they do? And what do we need to do to safeguard customer loyalty?

The big tech expansion into financial services has been a natural evolution. Tech giants like Microsoft, Amazon, Google, Apple, Facebook, Alibaba and Tencent are among the 10 largest companies in the world, and they all owe their success to their strong, data-driven customer focus.

By leveraging this data these companies can create ever more relevant, personal and intuitive experiences

for users, leading to a level of engagement that allows them to quickly move into (and take over) new industry segments.

Over the last decade, we've seen big tech introduce payment services – and slowly move into credit, insurance, savings and investments. They're already making headway in that space in the US and China, and are now setting their sights to the open banking opportunity in Europe.

These are the three paths we think big tech could take to venture into the European market:

### 1. Enhancing existing services

While we wouldn't be surprised to see big tech launch money management apps alongside what they already do, there could be a more significant impact if people's



financial information gets added to the apps they already rely on every day.

This strengthens the big techs' offering, as it makes their products (something people already use) more useful, rather than trying to change behaviour or sell a new service.

For instance, your account transactions could appear on Google Maps, pinpointing when, where and on what you spent money. Your past spending habits could be used to help personalise search engine results. Soon, you might simply be able to ask Alexa, Siri or Cortana to tell you how much money you have left to spend this month, ask them to set a spending budget, or even action a payment.

We know that big tech excels at creating compelling user experiences, so if they also have a PSD2 licence that lets them access bank account information or initiate payments, the options to enhance the digital services millions already love are vast.

## 2. Taking over the customer relationship

The rise of digital wallets gives big tech a big opportunity to take over the relationship between consumers and financial services providers.

These services don't only gather people's different bank accounts and credit card information in one place, but then lets users make payments from any of these accounts through one app – online or in person.

This means that, with a digital wallet, people no longer

have to carry physical credit or debit cards, or log into separate banking apps to make payments. It would all be done in the tech giant's existing environment.

If big tech can provide a real-time view of people's transactions and account balances in one digital wallet, it means people would have much less engagement with their bank or card provider. The big tech is effectively squeezing itself between the two and winning the customer's exclusive attention. The entire payment process would be hugely streamlined and simplified, in a digital environment the user

has already bought into.

As the number of point-of-sale systems that accept contactless payments grows, so does the threat of a big tech takeover of the customer relationship.

## 3. Displacing financial service providers

As consumers and merchants both become increasingly comfortable with cashless payments and digital products, we could see big tech start to offer their own brand of financial services.

Given that they operate some of the biggest online marketplaces in the world, it seems inevitable that big tech will take their first step towards replacing some primary banking services entirely – by creating their own payment systems that reward users for their loyalty.

One solid example is [Apple Card – going live in the US this month](#), and with a European launch expected to follow. It comes with zero fees, gives users daily cash-back on their spending, and helps people manage their payments to avoid interest charges.

Big tech's position as a financial provider could become even more powerful when the ability to make payments is combined with services like integrated billing and digital receipt management, both online and in physical stores. Or even by moving into areas such as offering cash advances or insurance.

When highly competitive products can be delivered on a slick platform that the user already values, it could be tough for more traditional providers to match up.

## Staying ahead of the surge

So far, only Google has a licence to operate as an Account Information Service Provider (AISP) and a Payment Initiation Service Provider (PISP) under PSD2. Other big tech companies are rumoured to be testing APIs while they wait for the licence to have their status rubber-stamped.

And while big tech surge could mean anything from taking over the relationship people have with their banks to head-to-head competition with financial ser-

vices providers, one thing is certain: we can definitely expect to see a range of new financial services come to life over time.

As of now, the advantage is still on the banks' side. They are still closer to the customers and have already established a relationship with them. To stay ahead of the big tech surge, banks will need to beat these companies at their own game: focusing on customers and finding ways to add value for them through personalisation.

Source: [Tink](#)

# The California Consumer Privacy Act (CCPA) The Top 5 Things Every Merchant Needs to Know

Privacy has been and will continue to be a major focus for regulators around the world. With data breaches and incidents showing no signs of abating, businesses need to ensure that principles of privacy and the protection of personal data are embedded into company culture or risk facing the consequences.

The California Consumer Privacy Act (CCPA), which becomes effective on January 1, 2020, marks a shift in the US regulatory landscape for privacy. CCPA aims to provide Californians with the following rights:

1. To know what data is being collected about them;
2. To know if their personal information is being "sold," as defined in CCPA, and to opt out of that sale if so;
3. To access the information collected about them by businesses; and
4. To equal treatment in the event they exercise their privacy rights.

This law will have a significant impact by any measure.

An independent report prepared for the Attorney General in August 2019 estimated that firms may have to pay up to \$55 billion in initial compliance costs. In order to help merchants better prepare for impending CCPA regulations and to better understand what it may mean for their businesses, I wanted to address the the top 5 questions I've heard most often.

## 1. Why is the CCPA a significant piece of legislation?

The economy of California is the largest in the United States with a gross state product of \$3 trillion in 2018 – as a sovereign nation, California would rank as the world's fifth largest economy. As a result, any companies doing business in California and nationwide will be impacted.

Its scope is also wide, which means that any significant business selling to California customers should assess CCPA's applicability. The law also has wider ramifications across the United States: CCPA provides a template for other states to create analogous privacy legislation, and

it may serve as the impetus for a federal privacy law. Finally, the costs of noncompliance could be extremely high, ranging from California Attorney General enforcement and civil penalties, to private suits and class actions, to reputational harm and loss of customer trust.

## 2. Is this law similar to the EU's General Data Protection Regulation (GDPR)? And if so, are there any lessons that could be applied to CCPA?

Some have referred to the CCPA as "GDPR lite" due to similarities between the regulations, but there are important differences and compliance requirements. For example, CCPA has a broader definition of personal data (including inferences and probabilistic identifiers), stricter notice requirements, different application



of the "right to delete" concept, and an opt out for the "sale" of personal data.

As in any compliance initiative, context is key. For each arm of an organization, the questions posed by CCPA are the same. But the answers may be very different for data processing activities supporting marketing vs. finance vs. fraud and security. In particular, both CCPA and GDPR contain specific provisions acknowledging that privacy regulations may create vulnerabilities in a fraud prevention program if appropriate accommodations are not made. Accordingly, it is critical that privacy teams managing enterprise-wide compliance programs are sensitive to context-specific concerns around fraud and security.

## 3. As consumer awareness around personal data and privacy increases, do you think regulations like CCPA will help to build trust in online transactions?

Privacy and security need to be top of mind for any company collecting, processing, or using personal data. As consumer awareness grows, and as legislatures and regulators respond to the increased focus on this issue, businesses will need to adapt and respond as laws, consumer expectations, and enforcement practices change. The only effective way to prepare for this evolving landscape is to embed principles of privacy and security into all of a business's operations. While this may involve up-front investment, it will pay off in the long term by securing customer trust.

## 4. What impact may this have for online merchants?

Clearly e-commerce and online merchants selling to California consumers will need to assess the impact of CCPA on their operations. If a merchant has conducted a GDPR compliance audit and implemented a compliance program, much of the infrastructure needed for CCPA compliance may already be in place.

## 5. What can merchants do to best prepare for CCPA?

Here are some practical first steps to address CCPA compliance for your business:

- Privacy Policy Management: Update privacy policies to reflect CCPA compliance
- Data Lifecycle Management: Create a data map and update data inventories
- Privacy by Design: Embed privacy and security at the earliest stage of product development
- Individual Rights: Implement a compliance program to enable the individual rights provided by CCPA
- Information Security: Ensure the security program is industry standard or better
- Data Processors: Review contracts with service providers and ensure accountability
- Training and Awareness: Update or implement training programs for CCPA-specific processes

Author: Scott Buell, General Counsel, Forter  
Source: [Forter](#)

# Industry interviews



## Ruca Sousa Marques CEO Switch

Speaker at MPE 2020, Berlin Feb 18-20

### **1. The Payment industry 2020: competition, pressure over margins from regulations and payment schemes: How do you view the payment industry now and in 5 years?**

As technology drives new business models and consumer behavior evolves, an expectation of fast, convenient, and secure checkout experiences emerges. In this context, payments play a cornerstone role in the path-to-purchase.

Merchants are increasingly concerned with low conversion rates through abandonment and declines (especially on mobile channels), risk/fraud through different attacks, and higher transactional costs for CNP versus CP. As remote commerce grows in popularity, so does regulators' and schemes' incentive to push new legislation/standards to address the excess risk involved in this transactional environment. Two main variables from the transaction flow are being affected by these initiatives: Transaction messaging and Authentication.

Initiatives in transaction messages involve adopting secure communication standards, such as the ones adopted for CP environments i.e. Cryptograms. Authentication is both being enforced but also evolving into easier and non-intrusive methods to validate account holders. This means interoperable standards that involve the digitisation of payment instruments for use across multiple channels, adopting a convenient authentication method e.g. biometrics. In this scenario, Authentication in CNP transactions becomes at least as secure as traditional Chip&PIN solutions in CP environments, and there will be no reason for the former to be more expensive than the latter.

In the end—with authentication solved—we'll move from a Card Present scenario to a Cardholder Present one, where location is no longer important: payments will transcend the physical world altogether. This trend will ultimately unlock new use cases, such as internet-connected devices and checkout-free stores, making the act of payment so frictionless that it becomes almost invisible.

### **2. How do incumbent companies fit into this system?**

In this rapidly evolving landscape, incumbent companies have bigger challenges ahead, especially due to technological constraints. Traditional software architectures have a hard time supporting a wider variety of frontends & channels, more data points, a wide range of business actors (e.g. partners, suppliers), and unstructured data formats. As a result, incumbent companies fail to adapt in a timely manner to new market conditions—or when using external providers—they're left with no choice but to operate without redundancy and be tied to the same pricing and services.

### **3. How can legacy systems be adapted to new market standards?**

I believe in adaptation as a means to evolve, rather than substitution. What I mean by this, is that there's value in existing legacy systems—they're still performing valuable actions! What's needed though, is to decouple traditional monolithic architectures into microservices set ups, ones that allow for interoperability between internal/external systems, thus accelerating integrations with 3rd party vendors for quicker go-to market strategies. For this matter, a middleware is necessary to orchestrate communications through standardised data

structures, avoiding any updates in back-office systems every time a new application is connected.

**4. Value added service are crucial to maintain sustainable margins: through which VAS can this be achieved? How can payment providers unlock additional value?**

Consumer trends are pushing merchant demand, which in turn convert to business opportunities for PSPs. I see a couple trends unfolding, which can be grouped into

two main strategic axes:

- Acceptance: Enabling commerce on a global scale by adding local payment schemes, adopting emerging standards (e.g. EMV 3DS; SRC), and supporting new payment flows (e.g. Post-Payments; Credit to Consumer).
- Costs: Supporting provider redundancy (e.g. tokenization; transaction routing), adding Fraud Detection Technology, and local PSPs for interchange optimisation and multi-currency settlements.



# Jeremy Nicholds

## CEO

### Judopay

Speaker at MPE 2020, Berlin Feb 18-20

**1. What is the story behind your company? What is the company's purpose on the market and what challenges does it seek to address?**

Founded in 2012, Judopay is a recognised leader in mobile-first payments. Born out of a frustration with clunky, friction-filled checkouts we built a fully native, customisable and seamless solution designed to drive merchant sales and reduce cart abandonment rates. Today, Judopay is the trusted mobile payment partner for global brands such as KFC, and a host of other food & beverage merchants, transit merchants, financial services and digital disruptors like JustPark.

Technology is evolving at a rapid pace; that's nothing new. In 2019, m-Commerce will constitute c.56% of all e-Commerce sales, with an estimated \$3.6trn in m-Commerce sales by 2021.

Mobile technology has changed the world. Customers' expectations have dramatically changed and payment technology has struggled to keep up. Currently, only 20% of merchants have a mobile payments app and only 40% have a mobile-centric payments website.

Developing mobile-centric technology, where payments are fast, secure, and convenient and engaging is what Judopay is about. Our mission is to create the best payment experience for our customer's customer and get commerce on the move.

**2. How can payment leaders best make the business case for new payment technology investment?**

The true value of a high-quality payments solution is often ignored. As long as a business is just concerned with processing payments they're content - but, start discussing international expansion, reducing fraud, increasing authorisation rates and suddenly the business case for innovative payment technology becomes clear. If you're looking to build a case for technology investment, explore your business' growth goals and how this new payment technology can support these plans.

**3. What's the single most dramatic shift you see happening in the merchant payments space today?**

Aside from the shift towards cashlessness, the develo-

ment of a subscriber economy has made a huge impact in both the retail and payments space. Merchants such as Zipcar, Spotify and Adobe are seeing consumers opt for a lower recurring monthly payment rather than forking out a much higher outlay to own the product/service. For me, it's a great example of how consumer demand can shape the payment landscape.

#### **4. How are new payment related technologies changing the way people pay today?**

Consumers want to be able to consume when they want, where they want. They want payments to just

happen, to be subliminal - the issue with online shopping in the past is, it's been fraught with friction - having to overload on information input, adding delivery details, billing addresses and card numbers - All this delay gives customers ample opportunity to drop off or decide better against buying that Christmas jumper.

New payment technology such as the launch of one-click payments has removed more barriers to purchase making online payments a more seamless and emotion-based transaction. New payment technologies are taking out the friction of online shopping and making retail therapy actually therapeutic.

# Martin Sweeney

## CEO

# Ravelin

Speaker at MPE 2020, Berlin Feb 18-20



#### **1. Payment fraud is becoming more complex and expensive. How will fraud attacks evolve in the upcoming 3-5 years?**

The good news is we're already seeing businesses getting better at preventing fraud. As more organizations make the switch to machine-learning solutions, this will help improve their ability to stop fraud impacting their business. On the other hand, we know that whenever we close off an opportunity in one area, fraudsters look elsewhere to try and create new, sophisticated methods of attack.

Account takeover is already growing at an alarming rate and I expect this to continue. This is when a fraudster gets access to a genuine customer's account and uses it to make fraudulent orders, take advantage of stored credits or extract customer details.

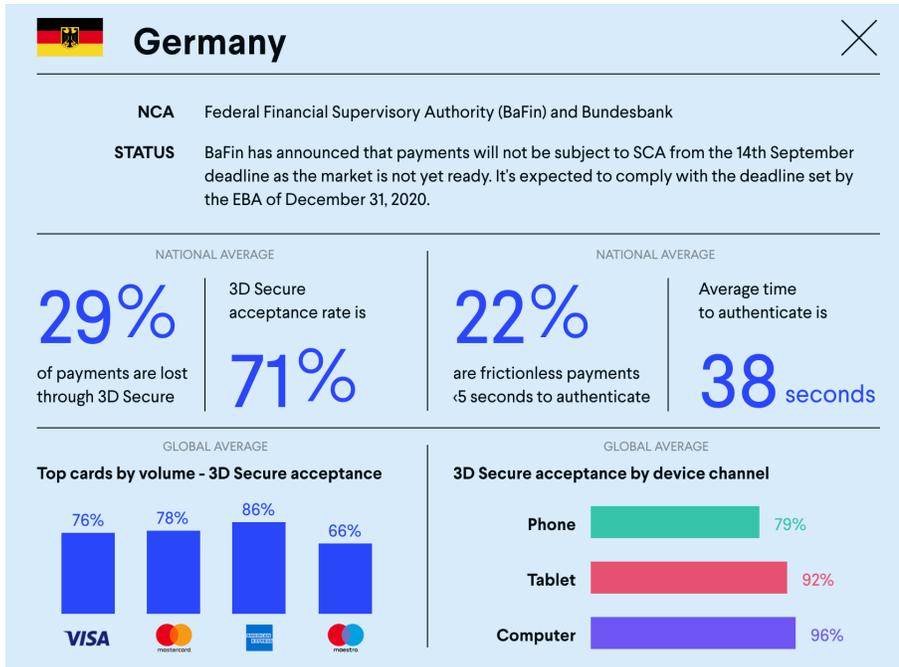
Account takeover is a result of a combination of data breaches, password reuse, and customers' ability to store their payment cards on merchant accounts. Many

organizations are only now starting to realize the reality of this risk, and so the response has been slow. Leading merchants need to get ahead of this problem before they suffer an attack in the public eye or a hefty fine relating to GDPR.

Right now, we're seeing a trend towards regulation promoting more payment authentication, such as within PSD2. Added security measures may make it temporarily more difficult for fraudsters to get results - but as we know, fraudsters often find ways to exploit these measures for their gain. I expect the increased use of 3D Secure will open up the possibility of phishing attacks, possibly 3D Secure spoofing by fraudsters to use this to their advantage.

#### **2. What do you recommend merchants do to get ready to defend against new and evolving types of fraud attacks?**

The most important thing to focus on is your data. Get this in order immediately - if you can't see clearly what's



2% of the 978 million global victims of cybercrime and almost 4% of the global losses.

What's interesting is that across the globe there are varying levels of 3D Secure success - in fact, in some countries, a payment sent to 3D Secure is more likely to fail. There are a range of factors which can influence this, including the percentage of online payments made by card, whether there is a mandate for authentication and the development of the payments infrastructure. You can check out the differences in our [global online payment regulation map here](#).

I'd encourage merchants to pay close attention to how the location of the issuing bank affects the success rate for 3D Secure. With Ravelin Accept, we give merchants reports on 3D Secure acceptance by issuer country and automatically choose the best route of action for each payment depending on the individual issuer.

happening in your business, you can't raise awareness and understand how to stop it. A company's data is its most valuable asset, but few have the skills and resources to understand how to use it effectively.

Therefore, my advice is to work with a partner who has the resources and expertise to help you. For large enterprises, this means working closely with your fraud partner rather than relying on a payment provider to take responsibility for your fraud. It's likely you'll need to work with more than one payment provider, which makes it more effective to do the risk analysis and manage your fraud protection yourself. You have the most data on your customers, transactions and the fraud you're facing. This puts you in the best position to derive the insights and results you need.

I also recommend sharing knowledge when it's appropriate. Since we founded Ravelin we've seen a huge increase in collaboration between merchants, which is fantastic. We wholeheartedly support this and try to contribute through participating in industry events like MPE, hosting our own events and creating merchant-led content.

**3. What insights can you share with MPE community regarding current fraud challenges across different countries and verticals? (Support your answer with an infographic, internal research or diagram)**

It's no secret that certain global regions are more well-known for fraud, for example South America, but it might surprise you that Brits represent a disproportionate amount of cybercrime victims - despite making up just 1% of the global population, the UK accounts for

**4. What does Ravelin mean? What is the story behind your company name and logo?**

A ravelin is a fortification on a mediaeval fortress. We wanted to imply "secure, safe, defensible". Our designer came up with a star fort as our logo that incorporated several ravelins.

**Feedback on what now needs to happen to make the transition a success?**

Since the EBA published the final deadline of 31/12/2020 for SCA, your PSD2 activity may have slowed down and started to look a little dusty. It's now time to re-energise your PSD2 preparation so you are ready when changes come into effect. Make sure your out-of-scope transactions are flagged correctly and avoid making customers jump through hoops if they don't need to.

It's critical for merchants to manage their own Transaction Risk Analysis. This actually benefits payment providers, as merchants have more data to make a decision with. I also advise merchants to start collecting intelligence on how issuers are managing authentication well ahead of the deadline. This will help you to help you react to real-world actions and changes in behaviour fast.



# Global Statistics

GLOBAL AVERAGE

30%

of payments are lost through 3D Secure

3D Secure acceptance rate is

70%

GLOBAL AVERAGE

6%

are frictionless payments >5 seconds to authenticate

Average time to authenticate is

41 seconds

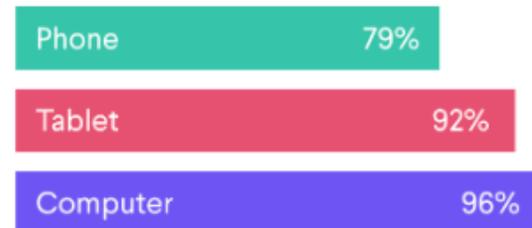
## Top cards by volume - 3D Secure acceptance

GLOBAL AVERAGE



## 3D Secure acceptance by device channel

GLOBAL AVERAGE



## Top 3 payment methods for digital purchases



36%  
eWallet



35%  
Credit/Debit card



11%  
Bank Transfer

# Fraud Prevention and Online Authentication Report



The Paypers' Fraud Prevention and Online Authentication Report aims to help the payments ecosystem to keep pace with the latest trends and developments, disruptive innovations, and fraud challenges. By capturing the views of experts ranging from solution providers, merchants, industry associations to consultancy companies, the Report depicts insights into risk management, data intelligence and machine learning, and how will fraud look after PSD2's Strong Customer Authentication.

Here is a sneak preview of this report.

## Fraud trends that shape a vulnerable environment

- Account opening fraud
- Authorised push payment fraud (APP fraud)
- Bad bot attacks

## Where is fraud heading after PSD2's SCA?

The blind side of SCA lies in the fact that fraudsters will turn their attention to out of scope transactions. According to CyberSource, fraudsters may try using non-EEA cards such as American card details, when targeting EEA merchants, or they can target non-EEA ecommerce websites with EEA card details. Online merchants are also advised to monitor the MOTO channels, because fraudsters will explore this option as well, by corrupting the call centres and impersonating genuine customers.

Juniper Research state in their article that the industry will witness emerging threats and new patterns in fraudsters' behaviour, while annual online payment

fraud losses from ecommerce, airline ticketing, money transfer, and banking services, [will reach USD 48 billion by 2023](#).

## Artificial intelligence – unboxed and upgraded

We learn from Feedzai that Explainable AI (XAI) is a machine that teaches by providing insights to teams. This way, fraud and risk management teams understand the reason an AI system makes a specific prediction or decision, or why it failed and how the errors can be corrected. Simility also emphasises the need for explainability, AutoML, and on top of all, the ability to adapt to customer demands, new fraud techniques, and regulatory environments.

## The smart use of data intelligence

Data is the new currency for both cybercriminals and businesses. While the former use it for malicious purposes, the latter use it to wipe out fraud and gather as much input as needed to improve the customer experience and to design robust risk intelligence. Merchants, banks, fintechs use data to create personalised services for their customers, but data is also key for solution providers that create fraud detection and prevention solutions. Data sharing is now a great practice to better detect friendly fraud, illegitimate chargebacks, account takeover, and other similar types of fraud through the collaboration of the entire community of industry players.

## Industry mapping of solution providers

This year, we have put together a more comprehensive mapping of players, enriched with new categories and capabilities (proprietary and via third parties), such as spam and abuse, bot risk management, decision orchestration, information sharing to name a few. We have welcomed on board companies such as Kasada, Forter, Identiq, Arkose Labs, Seon, G+D Mobile Security, and many more.

The Paypers team invites you to explore this Report to learn what's new in the fraud prevention and online authentication industry and what will influence this industry in terms of security, technology, and customer experience throughout 2020.



# Global payments made easy: Three Payment Tips To Increase Reach with Your Platform

Sponsored by:



So, you want to become a global leader with your platform or marketplace but don't have minions to do your bidding? And you are also not sure about the local payment options you should take into consideration to not miss out on opportunities? Fear not, we will provide you three important tips that you can use to "take over the world" or at least expand to another country or two. This webinar will provide you with tips on what you need to consider as you expand your empire:

- How to make transaction easier for global buyers
- How to make seller easier for foreign sellers
- How to establish your business to minimize risk and fees

## Speakers & Panelists



Andrew Whitcombe  
(Moderator)  
Principal Consultant  
Consult Hyperion



Matt Jackson  
Partner Manager  
PPRO Group



Keith Lam  
Sr. Director of Product  
Marketing  
Yapstone

[Download webinar here](#)

# 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](http://www.merchantpaymentsecosystem.com)

2010

Jan

 Square

## 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](http://www.squareup.com)

2010

Mar

 LightSpeed

## 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](http://www.lightspeed.com)

2010

Apr

 ShopKeep POS  
The simplest way to make smarter business

## Shopkeep

**Provider to merchants:** ✓  
(Core Service, Back Office, Front Office)

**Product Name:** Shopkeep