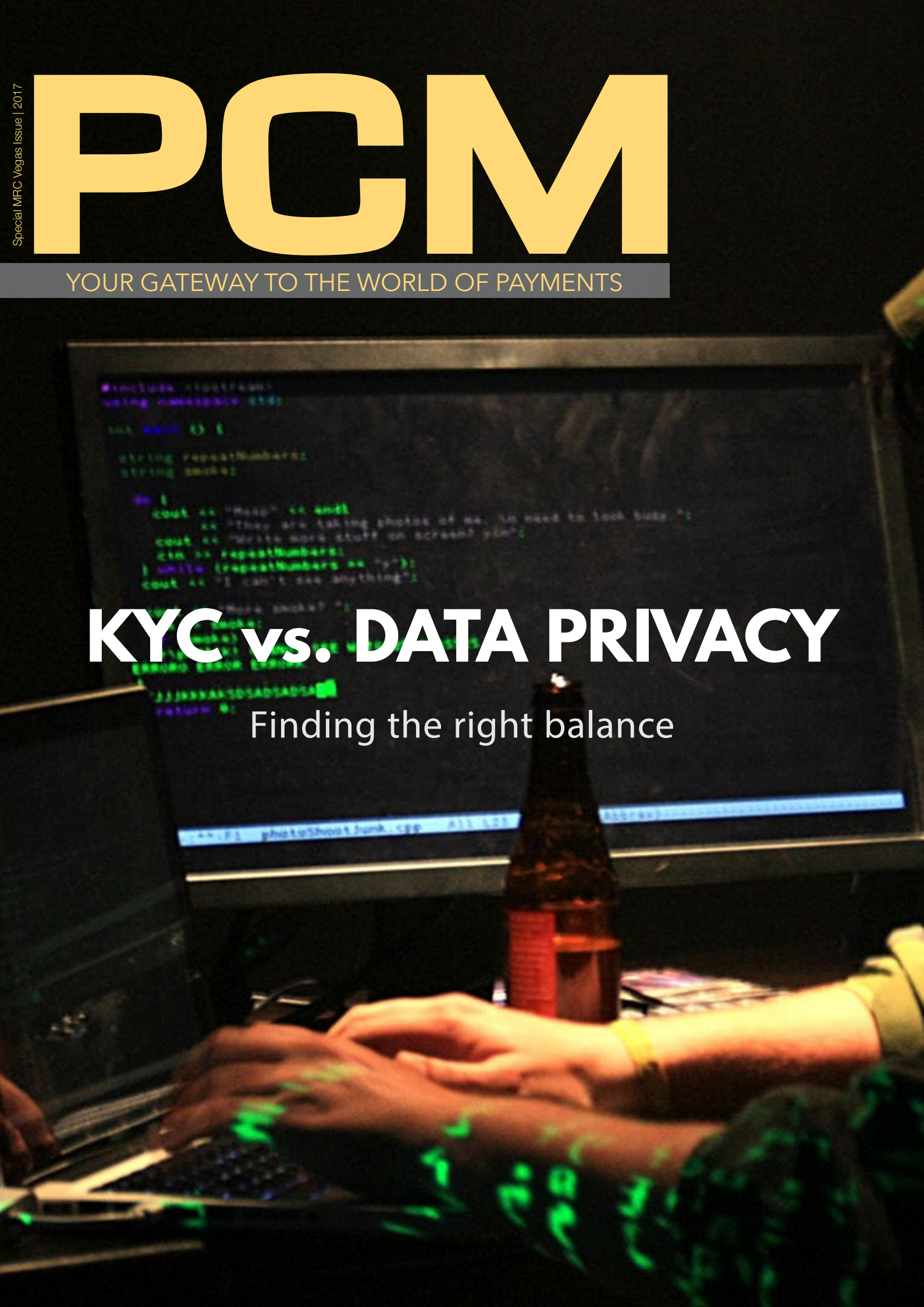
Special MRC Vegas Issue | 2017

PCM

YOUR GATEWAY TO THE WORLD OF PAYMENTS



KYC vs. DATA PRIVACY

Finding the right balance

DIGITAL SOURCE

CONNECTING YOU WITH THE PEOPLE TO POWER YOUR BUSINESS EFFICIENCY

CONTACT US NOW

Having data dilemmas? Please contact: **simon@digitalsource.io**

Digital Source | Herengracht 576 | 1017 CJ | Amsterdam | The Netherlands | +31 (0) 202 373 639

Payments & Cards Network

Amir Abdin
Editor-in-Chief
amir@paymentsandcardsnetwork.com
https://nl.linkedin.com/in/amir-abdin-21365683

Duc Dang
Production Editor
duc@paymentsandcardsnetwork.com
https://nl.linkedin.com/in/ducdanghh

Layla Durani
Editor
layla@paymentsandcardsnetwork.com
https://nl.linkedin.com/in/layladurrani

Contents

STORIES

4 Protecting business and customers: Meeting the modern anti-fraud challenge

7 Knowing your customer: Easing the tension between customer identity & privacy

9 The dry acronym that will change the face of banking

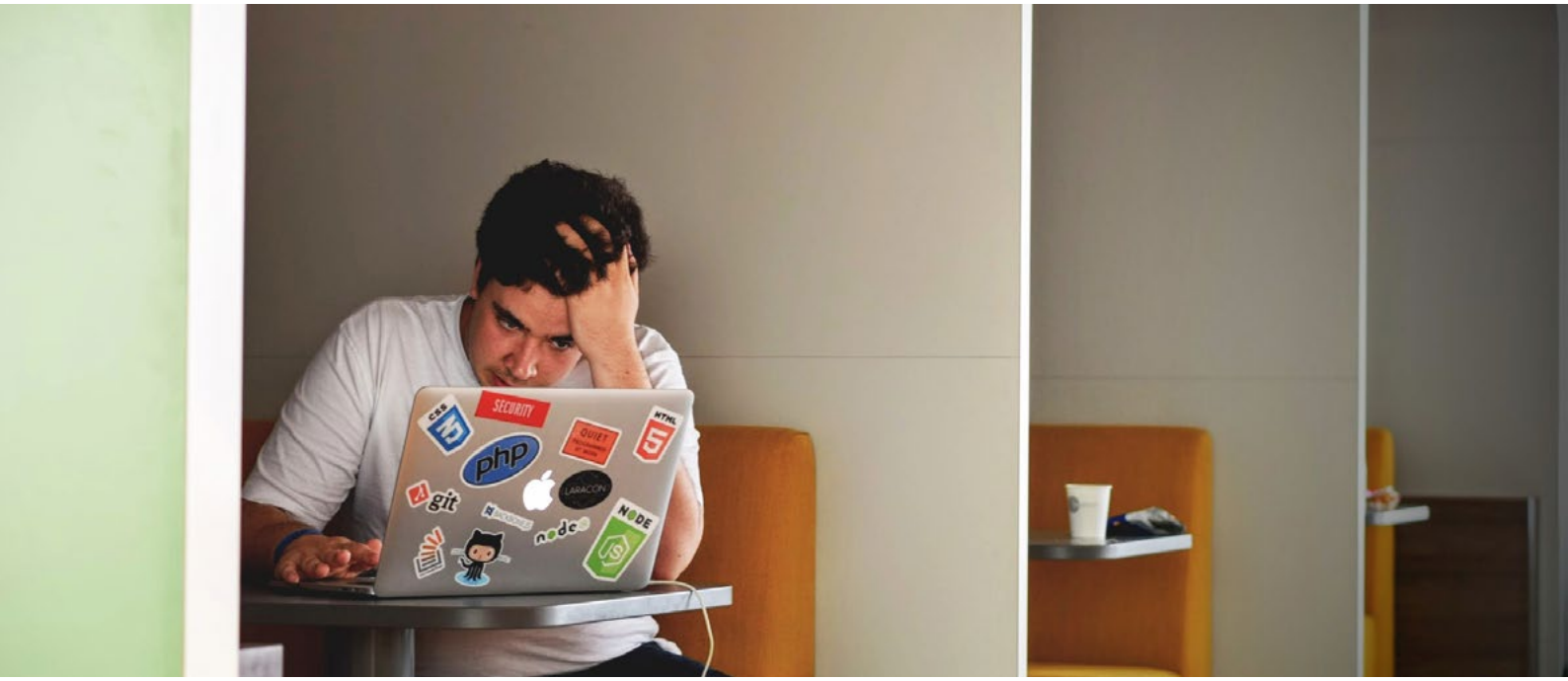
12 The route into the payments world

16 Start-up Spotlight: 4Stop

THANKS TO OUR PARTNERS

MRC Building Better Commerce
Fraud & Payments Professionals

mondato



Protecting business and customers: Meeting the modern anti-fraud challenge

by Roberto Valerio

Online customers have never been so vulnerable. A recent survey by Pew Research Center found that 16% of North Americans have had their email accounts hacked while 13% claim that someone has taken over at least one of their social media accounts. In total, 64% of respondents had personally experienced a major data breach and 41% had encountered fraudulent charges on their credit cards[1].

But why are these numbers so high? One reason is that we each have far too many online accounts and therefore too many details to remember. The average Internet user has more than 100 online accounts and the numbers are still rising[2]. People tend to simplify security measures by using easy-to remember-passwords. Unfortunately, easy-to-remember passwords also tend to be easy-to-break. Fraudsters are aware of this weakness and are only too happy to exploit it.

Online retailers have tried to encourage tougher security by rating customer passwords from weak to strong, but even if the customer is using a strong password, they may be using the same one across a plethora of accounts. This means that a fraudster who obtains the password for, say a simple lending library account, might also be able to access that user's accounts across fashion retailers, train operators, insurance providers, ticket sellers and more.

However, the most critical account is the email account. Email accounts typically act as the anchor for the user's whole online life. Once the fraudster has access there, they can re-set the passwords of other accounts and go on a digital foray, potentially making fraudulent orders across a lot of online merchants. Of the 100+ accounts many of us operate online, the majority are linked to just one email account[3]. Even if a consumer does try to make their passwords complex and secure, just one weak password can make them extremely vulnerable. A single account with a pizza delivery firm that was only used one time five years ago, but is protected by the password "123456" can be a huge weak spot. Fraudsters will target these discarded accounts to gather personal data and wreak havoc.

For those with strong digital security across their digital profiles, dangers still lurk. Fraudsters can gain access to these accounts using more sophisticated techniques. Phishing attacks, for example, have risen sharply over the past few years with an estimated success rate of 45% in obtaining usernames and passwords.[4] Malware can also be used to spy on computers and intercept login credentials.

The problem with account takeovers is that a genuine account offers fraudsters a significant advantage: trustworthiness. Online businesses will naturally place much more trust in existing customer accounts with years of good experience behind them, than they do with new customer accounts. This gives fraudsters space in which to hide and enrich themselves.

Looking to the future, we must prepare for how consumers are likely to secure their online lives in the connected age of

the Internet of Things. Already we have connected fridges that order food; cars that make automatic payments at petrol stations; and thermostats that make heating decisions based on the location of the user's phone. Cisco estimates that the number of machine-to-machine connections will grow by 250% between 2015 and 2020. We can also expect the number of internet users to grow from 3 billion to 4.1 billion by in this time. As the internet grows with more people and more devices, so too do the entry points for fraudsters.

The online threats we all face today have never been greater or more sophisticated. Many of us access the internet through a multitude of devices and accounts. But how can fraudsters be tracked down? The problem is that fraudsters have become very adept at covering their tracks and masking their identities. So vendors need to step up their game as well. New fraud prevention software uses Machine Learning technology to adapt instantly to the constantly changing patterns within fraud. It takes the pressure from the merchants to keep their traditional rule sets up-to-date on a daily basis.

One thing that is certain is that fraudsters will not stop evolving their techniques. Many run professional-type organisations whose sole purpose is to steal, sell, manipulate and use customer data to commit fraud for easy financial wins. The challenge for the rest of us to stay one step ahead of them. Anti-fraud engineers will continue to innovate new technologies that work alongside knowledgeable fraud managers to provide the best defences for merchants. Merchants will continue to push for the greatest security available so they can protect their customers. And customers must ensure they do not make it easy for their accounts to be compromised.

Risk Ident

Risk Ident is a leading software company that offers efficient anti-fraud solutions to companies within the ecommerce, telecommunication and financial sectors - empowering fraud managers with intelligence and self-learning machine technology to provide stronger fraud prevention. The company is home to a veteran team of data scientists and software engineers with long-term experience in data analytics and machine learning. Risk Idents products are specifically tailored to comply with European data privacy regulations. www.riskident.com/en

[1] http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

[2] http://www.itproportal.com/2015/07/23/we-all-have-too-many-online-accounts-and-cant-remember-the-passwords/ org/2017/01/26/americans-and-cybersecurity/

[3] https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/

[4] https://www.itgovernance.co.uk/blog/google-study-phishing-attacks-work-45-of-the-time/

Come & Meet us at the MRC Vegas

You can find us at booth #209!

Roberto Valerio

CEO - Risk Ident GmbH

Roberto Valerio is founder and CEO of RISK IDENT, a software development company specialising in fraud prevention and credit risk evaluation based on machine learning. He plays an active part within the fraud prevention community and he is a member of the European Advisory Board at the Merchant Risk Council. Beforehand he founded and worked within different management roles for software startups. He has a background in business administration.

RISK IDENT

We're a global payment provider processing more than 2bn € annually across 150 countries and 220 payment types. By harnessing data analytics we help deliver valuable customer insights that enable our clients businesses to succeed.

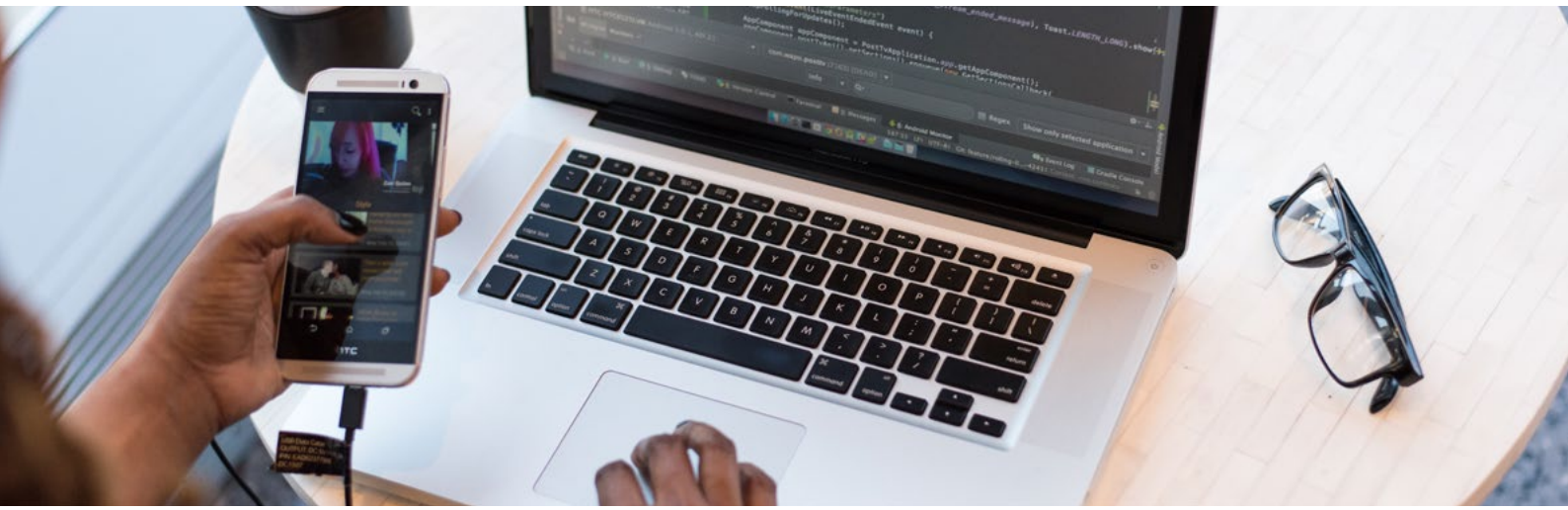
GLOBAL PAYMENTS

360 DEGREE CUSTOMER VIEW

OPTIMIZED CONVERSION

COMPREHENSIVE FRAUD PROTECTION

hipay.com



Knowing Your Customer: Easing the tension between customer identity and privacy

by Philip Atherton

Meeting Anti-Money Laundering (AML) rules and following Know Your Customer (KYC) guidelines isn't just a headache for payment providers. Getting it wrong could have serious consequences.

In opposition to this need to know exactly who a customer is to meet increasingly stringent regulations, customers are demanding that they keep their details private. One survey by the Information Commissioner's Office in 2016 showed that only a quarter of people trust businesses with their data. This lack of trust is either a desire for anonymity - perhaps a reaction to purchasing decisions leading to direct marketing that they find intrusive – or keeping details private to avoid being one of the millions of people who have had their details leaked in a security breach.

There is an unavoidable tension between regulations and the demands of customers.

Payment transformation

The emergence of mobile, the continued shift towards digital and instant payments, the rise of cryptocurrencies, and the wide-ranging impact of various regulations has precipitated the biggest transformation in payments since the advent of the internet.

As well AML/KYC regulation, mobile payments are becoming increasingly popular enabled by a new generation of mobile phones. Many mobile phones can now read a consumer's fingerprint and authenticate a consumer's identity, giving merchants and payment providers far greater confidence in the authenticity of the transaction. Payments can also be tied directly to a consumer's account on the merchant side, and associated to all the information provided to them.

This mobile technology may come in useful given the recently announced EBA rules on Strong Customer Authentication (SCA) which will demand that every online and unattended transaction in Europe over €30 must be subject to SCA – essentially two-factor authentication – with some exceptions. Add to this mix the increasing proliferation of digital ID schemes across the globe, it means that payments, and the audit trails that help regulate these payments, are changing quickly.

But consumer demand for privacy is also changing how payments are made. Bitcoin's anonymity is major factor in its popularity. However, with Bitcoin or any other cryptocurrency, there is a lot of doubt as to how this will fit in highly regulated markets as anything other than an investment vehicle. In fact, without systemic changes to the way Bitcoin, or other similar cryptocurrencies operate, it's highly unlikely that they would ever be accepted by the regulators responsible for European markets. This potential for misuse, as it's practically impossible to know where funds are coming from, is too high.

Knowing your customer – when they don't want you to know

It's clear that regulators require, and will continue to promote, the proliferation of highly-authenticated methods of payment in the future, with a clear audit trail. However, the very existence of cryptocurrency indicates a desire among consumers for a kind of payment system which lets them remain anonymous.

About Philip Atherton

Chief Risk Officer @ SafeCharge

Mr. Philip Atherton is the Chief Risk Officer at SafeCharge. Prior to joining SafeCharge, Philip served in various senior managerial positions in the card and payments industry at leading payments companies, Worldpay and Barclaycard. Philip's extensive experience in cards payments, risk management and regulation compliance has enabled him to build and manage teams, deliver significant incremental value through effective contract negotiation, provide tight control of compliance frameworks, execute revenue building strategies and have an in-depth understanding of the regulatory environment.

There are a number of reasons why this anonymity and privacy is important to many consumers, not just those who obsess over privacy and do their best to remain 'off the grid'. Data breaches, both in the ecommerce sector and outside it, have shaken consumers' trust in keeping data safe. Aside from convenience and choice, one of the biggest drivers of online payments is that people can pay for goods and services they may not be comfortable paying for on the high street – a data breach could leave them exposed. People are simply wary of giving away their details online, knowing that it exposes them to fraud and identity theft. Simply meeting AML/KYC regulations could lead to abandoned transactions and ultimately lost revenues as people choose to protect themselves rather than open themselves to more risk.

GDPR will help – but education will help more

The new General Data Protection Regulation (GDPR) rules due to come into effect in May 2018 may help put consumers' fears at rest. These rules will address concerns over the data held by companies, including data held on their payments. Consumers will be able to request details of what information is held about them, and also request that it is deleted if it no longer needs to be held for regulatory reasons.

These regulations can give consumers a better understanding of how their data is used and held by providing transparency. However, as an industry this is just part of the solution. For consumers to trust that their data is safe, there needs to be far better consumer education on how far the payment industry goes to ensure that these details remain safe and how they can help protect themselves.

There is a general reluctance in the payments industry to fully educate consumers on their rights and the provider's obligations, with the burden seen to rest on the consumer. But if consumers had a much greater understanding of what PCI compliance meant for their data, they would be much more willing to trust their data with someone who is accredited. Even concepts such as tokenisation should not just be jargon used by the payment industry, but a more widely-understood term that gives consumers an understanding of how they are protected, even in the case of a data breach.

Educating consumers in complex payment technology is not simple – trying to explain PCI compliance and tokenisation to people who just want to pay for something isn't easy. But letting customers know that their payment is protected according to certain standards, and that certain parties do not have access to full customer details, could go some way to meeting the need for privacy and anonymity. A customer more relaxed about a transaction is one that is more likely to go ahead with it, easing the tension between identity and privacy.

SafeCharge

SafeCharge is a global provider of technology-based multi-channel payments services and risk management solutions for demanding businesses, with operations in the UK, Guernsey, Cyprus, Bulgaria, Israel, Italy, Austria, Singapore and Hong Kong.

SAFECHARGE

The dry acronym that will change the face of banking

The European Commission's revised payment services directive brings threats and opportunities. What will be the attributes needed to survive and prosper in this new, open world, asks Peter Jan Van De Venn, chief commercial officer at Dutch digital banking solutions provider, Five Degrees.

by Peter-Jan van de Venn

PSD2 sounds technical and bland, like any acronym. It has hardly registered beyond the banking, fintech and payments sectors. However, the European Commission's revised Directive on Payment Services could have a seismic impact on customers' interaction with their banks.

It opens up Pandora's Box. Banks are required to provide access to account data to third parties at the request of customers. Additionally, the related General Data Protection Regulation (GDPR) requires banks to ensure the portability of their customer data.

As we move towards what is now commonly touted as "open API banking", PSD2 is expected to be a catalyst for unprecedented customer-oriented change. It constitutes an entirely new legal structure for payments across the EU. It will bring opportunities for banks and fintechs but they will need to amend their operating, business and revenue models, as well as the technology that supports these.

In response to PSD2, banks face fundamental choices. Do they become merely utility providers or the 'orchestrating hubs' to facilitate customers, services, providers, and payments? There will be new alliances and the winners will be those with greatest control of their capital and of the touch points on the customer journey, plus corporate and technical agility. Indeed, technology will be at the forefront and will be the differentiator between those that can take advantage of the opportunities and those that will be threatened.

Most interesting will be those banks that decide to set out their stalls as orchestrating hubs for all kinds of financial services across a huge marketplace. They will position themselves as trusted go-betweens for myriad services that can be added, modified or deleted at will.

This has given rise to the phrase 'marketplace banking', the concept of a bank acting as a go-between and as the hub for all kinds of financial services, each of which can be easily coupled or decoupled. To put it bluntly, the new bank is a bustling bazaar bringing together a world of services to serve each particular need of any type of customer at any point in time.

This puts new pressures on the underlying technology platform, with a prerequisite being seamlessly interconnected open APIs. This is not just about connecting to the outside world but also about opening up internally through APIs to provide access to a bank's own services. Key elements will include a digital banking platform that allows a high level of automation through workflow management and a service and integration layer to connect to third parties and to allow those third parties to connect to the bank's platform and services. All backed up by reliable, up-to-date, all-encompassing data.

According to Gartner, digital leaders and CIOs in EU-based banks should also use the introduction of PSD2 to upgrade their digital banking capabilities to fundamentally now support the expectations of their most sophisticated customers, thereby going well beyond mere cosmetic changes. Tying together and coordinating everything will be technology solutions that facilitate orchestration and unlock the ability of banks to become hubs within fintech ecosystems and within their own traditionally monolithic, siloed and often batch-oriented IT landscapes.

One bank that looks well placed in the Netherlands for the changes is Knab. By virtue of being a relatively new entrant, it was able to adopt a clean, three-layer architecture from the start, with Five Degrees' Matrix in the mid-office, as that orchestration layer and supporting customer relationship management (CRM), business process management (BPM) and document management. This will aid the bank as it introduces what René Frijters, Knab's founder, calls a "financial platform strategy" whereby Knab offers third party products in different areas where the match between the customer's profile and the third-party product should be optimal for the customer. It currently offers mortgage products from 28 different suppliers and will increasingly do the same in other areas.

As well as the technology challenge, there is also a cultural one. A bank's management will need to be honest about its strengths and weaknesses. Where the competencies of partners add value, they should be leveraged to improve the total product portfolio for the sake of client service delivery. There needs to be a shift from assuming that everything is best built in-house.

Taking again the example of Knab, which was the first digital,

About Peter-Jan van de Venn

Chief Commercial Officer @ Five Degrees

Peter was previously a consultant at Atos Consulting where he supported tier one banks with their IT management and strategy challenges. Subsequently he set up a consulting practice focused on the pressing need for banks to improve their digital transformation. He joined Five Degrees in 2011 and has held positions around project delivery, strategy and sales. As Chief Commercial Officer, Peter-Jan is responsible for marketing, sales and partner management within the company.

branchless retail and SME bank in the Netherlands, it is seeking to better serve the funding needs of its SME clients. Knab decided to connect to an external crowdfunding provider instead of creating its own loan products here. This required courage from management to use competitor products. However, Knab's management understood that using the marketplace for additional products allows the bank to keep close to its customers.

Aggregating all financial information in one place provides great cross-sell opportunities. This makes PSD2's Account Servicing Payments Service Provider (ASPSP) element particularly attractive to comparison websites. Customers will only need to enter their bank account login details for the ASPSP to access their account via API. The benefit to customers is clear: all accounts can be consolidated in one place.

Incumbent banks do have one competitive advantage: they still 'own' the customers' bank accounts whereas fintechs typically have the technology, the vision and the entrepreneurial spirit. Marrying the two sets of strengths makes sense.

Indeed, PSD2 gives banks the opportunity to be proactive and gain a competitive advantage by embracing open innovation. Many of the most eligible fintech partners are already forging relationships with banks, triggered by the opportunities that arise from the new legislative standard. Looking for alliances is one way to ensure success in a financial world that is facing upheaval.

Recently, several banks signed deals with fintech players. UK-based Metro Bank, for example, forged a partnership with Person to Person (P2P) lender, Zopa, to expand its credit facilities. Other notable new partnerships include digital banking platform Moven announcing a deal with online services, Payoff and Commonbond, and German fintech bank, Number26, tying up with TransferWise, a P2P money transfer firm. Banks that arrive late to the party may have to get in line to see their proactive peers exploit their first-mover advantage.

For traditional banks, there will be plenty of concerns about operating in an open API economy. It will mean inviting in new competitors from all corners of the business universe, bringing with them new financial and non-financial services, new customer experiences, and disruption to the incumbent banks while creating a vast, Europe-wide competitive environment. Where there are threats, there are also opportunities, but only for those that move early, embrace innovation, refresh their technology and, perhaps most importantly, change their traditional mindsets.

Five Degrees

Five Degrees' Matrix is a next generation digital banking and orchestration platform for financial institutions, from start-ups to tier one banks. It is the leader in its domestic Dutch market and increasingly beyond here, in part driven by the emerging business challenges of PSD2. Five Degrees is a young, dynamic company that forges deep, long-standing partnerships with its customers.

five degrees™

The Route into the Payments World

Danielle Nagao, Chief Executive Officer of the Merchant Risk Council, has over 20 years' experience in payment processing, fraud prevention, financial planning and business development. Prior to the MRC, Danielle was Vice President of Financial Operations at Tickets.com, a subsidiary of Major League Baseball Advanced Media/ MLB.com. In her role at Tickets.com she managed global payments, fraud, loss prevention and investigations. Before joining Tickets.com she was a Manager at Deloitte Consulting where she led ERP implementations across multiple industries. During her years as a merchant member of the MRC, Danielle held many volunteer roles, including director roles on both MRC's American Advisory Board and Global Board.

The payments sector has many facades and in a era of unprecedented technological discovery and change it can be very overwhelming in the beginning. We spoke to MRC's CEO, Danielle Nagao, about her path into the world of payments and the career lessons she learned on the way of becoming a leader in the industry.

PCM: Danielle, with 10+ years in the industry, how did you initially get involved in fraud and payments? What did the road to CEO look like?

Danielle: What's funny is I fell into the industry almost by mistake. At the time, fraud prevention and electronic payments were in their infancy stage and there was no dedicated resource at my organization truly managing these areas. The only problem was that I knew nothing about managing payments and fraud; I was an accountant, I crunched numbers for a living.

As I began learning about the industry, a colleague recommended that I attend an MRC event. Upon attending MRC Vegas 2007, my intention was to gain technical skills that I was lacking, but what really resonated with me was the open dialogue I was seeing, even among competitors. I loved the interaction and wanted to be as involved as possible. Hungry for more knowledge and opportunities for collaboration, I immersed myself in the MRC. I started out by joining the US Conference Committee, then the American Advisory Board and finally moved on to the Global Board of Directors. For me it was an exciting time to be involved because payments and fraud solutions were rapidly advancing and I enjoyed being part of the industry's transformation.

Fast forward to 2014 when the Global Board was tasked with finding a CEO for the MRC. As long-standing member of the MRC, it was my opinion that it would make the most sense to have someone from a merchant background run the organization. I ran through a list of merchants who I knew were passionate about the MRC and, funny enough, my name came up on that short list. I have always believed that timing is everything, and this was a time in my career where I was ready for that next big challenge. With complete certainty, throwing my hat in the ring was the right decision. During my time as CEO I have experienced a tremendous amount of personal and professional growth.

PCM: What's the most fulfilling part of working for a not-for-profit company focused on eCommerce? What gets you out of bed every day?

Danielle: At the heart of the MRC is a community of highly diverse individuals who are passionate about fraud, payments, risk, cybersecurity and technology. As a prior member of the MRC, I know first-hand that we are a driver of best practices, benchmarking and continued improvement for the industry. When I listen to members describe success stories, I am inspired because I know that we are a part of that overall story.

I also truly enjoy the networking and collaboration opportunities that we facilitate. One of the best parts of my job is connecting people and watching these personal and professional relationships

grow over the years. I can't tell you how many people have told me that some of their biggest professional opportunities have developed as a result of their involvement with the MRC.

PCM: Why do you think that the MRC is a valuable resource to the industry?

Danielle: The MRC's mission is entirely focused on our members and their desire to make commerce safe and profitable. The MRC provides an environment where professionals can share information and build essential business relationships. In the last year, the MRC has increased its efforts to provide more networking opportunities outside of the 4 annual events. We now host several Connects events across the US and Europe which give more professionals the opportunity to meet one another and discuss relevant topics free of cost.

The MRC also provides a wealth of valuable educational resources. While our events are very successful, we realize that they only cover 14 days out of the entire year. At the MRC we are committed to providing support to our members all year around. We host weekly webinars, provide beneficial benchmarking data through global payment and fraud surveys and maintain a vast resource library of white papers, case studies and presentations.

The proof is in the pudding. In our most recent global fraud survey, we not only looked at current trends, but also how MRC members stack up against non-members. Our research shows that MRC members have 29% less fraud that non-members. It is clear to me that we are making a difference and that the tools and resources that we provide are adding value.

PCM: Can you name a person who has had a tremendous impact on you as a leader? Why and how did this person impact your career?

Danielle: My Managing Partner at Deloitte Consulting was a great mentor to me. I started my family while working at Deloitte which was a difficult transition to meet all my work responsibilities while simultaneously juggling family commitments. He had a unique understanding of the challenges associated with maintaining a work-life balance and was able to provide perspective. On a less serious note, he also taught me that I should never take on the responsibility of ordering food for working lunches unless I wanted my colleagues to think of me as their mom.

PCM: What is one characteristic that you believe every leader/decision maker should possess?

Danielle: I believe the most valuable quality a leader can have is soft skills. We live in a very technically driven world and, in this industry, there is an expectation that you are technically savvy. In my opinion, technical skills are easier to learn than interpersonal skills. In today's environment, we replace text messages and emails for real conversations. We all know that those hard conversations are a lot easier if you don't have to look someone in the eye. However, thoughtful communication, emotional intelligence and relationship skills are the key to being an effective leader.

Throughout my career I've learned that the "one size fits all" mentality does not translate as a leader. Being able to evaluate individual's needs and personality styles are critical in management. Relationships can make or break careers.

PCM: What advice would you give someone entering this industry?

Danielle: Well, of course my first response is that they need to be part of the MRC family! All jokes aside, I would advise someone new in the industry to find a mentor. Although there are more resources now than ever available to beginners, nothing is more valuable than learned and shared experience. A seasoned professional can convey an honest perspective regarding industry success and failure and connect you with a network of professionals.

PCM: What makes MRC Vegas unique from other trade shows and events?

Danielle: As a past merchant attendee of many different industry events, I always looked forward to attending MRC Vegas for a number of reasons. Over the years, MRC Vegas has undergone many transformations: the venue has changed, the exhibit hall has grown immensely, a Demo Theater was developed so exhibiters could showcase their solutions, the event has become completely digital, etc. But at its core, the essence of the event remains the same- connecting bright minds to develop relationships and continue building better commerce. Our event encourages competitors to talk with each other and share best practices because in the MRC Vegas environment, we are all on the same team.

Each year the feedback from attendees is that the size of this event is key. It is big enough to connect global professionals from all over the world, but intimate enough to offer real conversations that lead to beneficial relationships. Our focus for MRC Vegas is not quantity, but quality. We don't strive to be the biggest event in the industry, we strive to execute an event that allows our attendees to maximize their time with the right people. At MRC Vegas, attendees walk away feeling accomplished, well connected and excited to get back to their day job where they can execute what they learned at the event.

MRC

The MRC (Merchant Risk Council) is an unbiased global community providing a platform for eCommerce fraud and payments professionals to come together and share information. As a not-for-profit entity, the MRC's vision is to make commerce safe and profitable everywhere by offering proprietary education, training and networking as well as a forum for timely and relevant discussions. The MRC was launched in 2000 at the start of the eCommerce boom by a small group of industry professionals from leading consumer brands, with the ultimate goal of combating online fraud in the card not present space. Since its inception, the MRC has also added online payments to its portfolio, expanding its presence further into eCommerce.

Building
Better Commerce

Fraud & Payments Professionals

Spotlight

You think you have what it takes to start a business in a super-hot market?

PCM takes a close look at some of the most innovative and promising startup companies in the payment industry.

Ingo Ernst, Founder & CEO

"STAY COMPLIANT BY ADDING ANY NEW KYC SERVICE OR RISK RULES REQUIRED AS REGULATIONS UPDATE"

After a turbulent and unpredictable 2016, the global payments industry has its work cut out to prepare for a flurry of regulatory, legislative and policy reforms in the near future. Due to the requirement for banks and payment service providers allowing secure third-party access to accounts, it will require those institutions to make wholesale changes, not only to their technology and infrastructure, but perhaps also to their business models. We spoke with Ingo Ernst, CEO & Founder at 4Stop, a company that helps other businesses with fraud migitation and compliance for localised regulatory requirements.

PCM: Tell us about 4Stop. How did the idea come to be?

Ingo: All founding partners of 4Stop have a background in the payment and risk management space. Having worked in executive positions at acquiring banks, marketplaces and large scale e-commerce businesses there was a constant need to improve the compliance, anti-fraud and risk management features at every level.

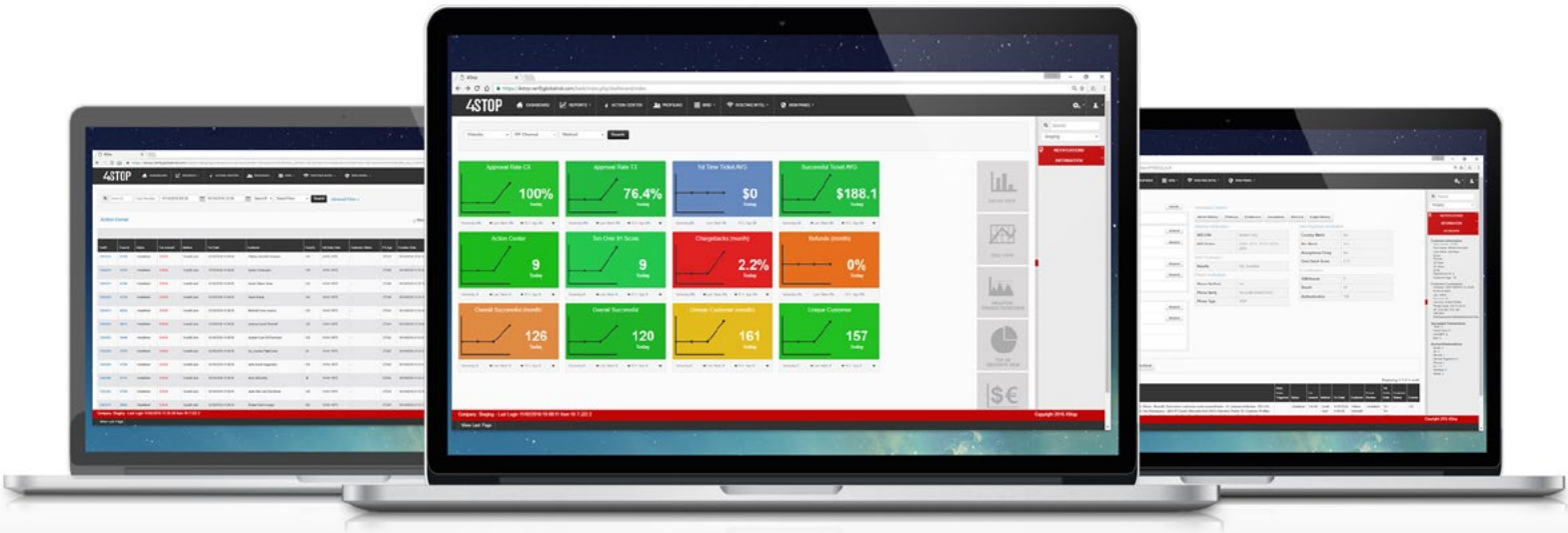
The primary obstacle in setting up a streamlined risk-based approach and a globally scalable set of data providers for compliant KYC procedures is the challenge of having to integrate various data provider at different touch points in the customer experience. Traditionally this has been solved by various API integrations, Backoffice Management Systems and the teams under our leadership applying a patchwork approach to establish thorough KYC or risk check on clients and transactions.

The founding members of 4Stop wanted to establish a solution. A single API integration that provided a sin-gle Backoffice Management System with robust flexibility to enable global data sources in real-time, coupled with advanced risk management tools such as real-time dynamic rule sets. We did not know what will all change in the coming years, however one thing was certain, that change will be on-going as the regulating bodies in the various verticals related to online payments continue to tighten their rules and regulations framework to move closer to a fully supervised and compliant payment ecosystem.

Establishing one product, one platform that not only simplifies and streamlines the risk management and compliance processes but enables enterprise-level businesses to process transactions globally with confidence and compliance as the regulatory and fraud landscapes change was our objective.

PCM: Why is it called 4Stop?

Ingo: When it came to branding our product we wanted a brand that resembled our marketplace focus, was memorable and knew no boundaries to 'trend-based' vocabulary. With that, 4Stop was established. The methodology of this brand name is multi-layered. Starting with the '4' not only representing the four founding members of the company but the four directions (North, East, South and West). With a product offering focused within the risk management space and combatting fraud, 4Stop speaks to protection. With our platform, we provide tools to stop fraud and manage risk from all directions and touch



points of a business transactional eco-system.

PCM: Why is 4Stop needed?

Ingo: Know Your Customer (KYC) for regulatory requirements continue to evolve both in the type of due diligence required and the level of complexity in which it is performed. Financial institutions (FIs), banks and their customers are constantly managing the ever-changing regulatory landscape and trying to find new streamlined and cost-effective methods to integrate changes when they occur. While compliance is not an option but a legal requirement, these businesses must integrate processes that satisfy the regulator while still delivering a positive customer experience.

One of the revised – and more stringent – set of requirements to prevent money laundering and the financing of terrorism is the 4MLD implementation, which will be required by no later than the end of 2016. The 4AMLD for the first time includes online operators, while it was previously just focused on land-based casinos. What was previously a best practice is now a regulatory requirement which has a severe impact on online operators everywhere. A good example for the increased scrutiny is a judgement by the UK Gambling Commission that had two gaming operators having to set aside £1.7M due to failing the AML regulations and rules. Fines now more than ever have a severe impact on the overall processing cost and have become a true factor in the overall success of a business.

That is just one of the many examples of the rapidly tightening and changing regulations. 4Stop is seeing a large demand for hands-on expertise from true compliance specialists that bring together knowledge of the acquiring and processing world, compliance and regulatory background coupled with vast experience. A rare skill set combination required to keep up with today's compliance regulations and have a future proof set-up to avoid fines or even worse - being shut down for non-compliance.

PCM: What makes 4Stop different?

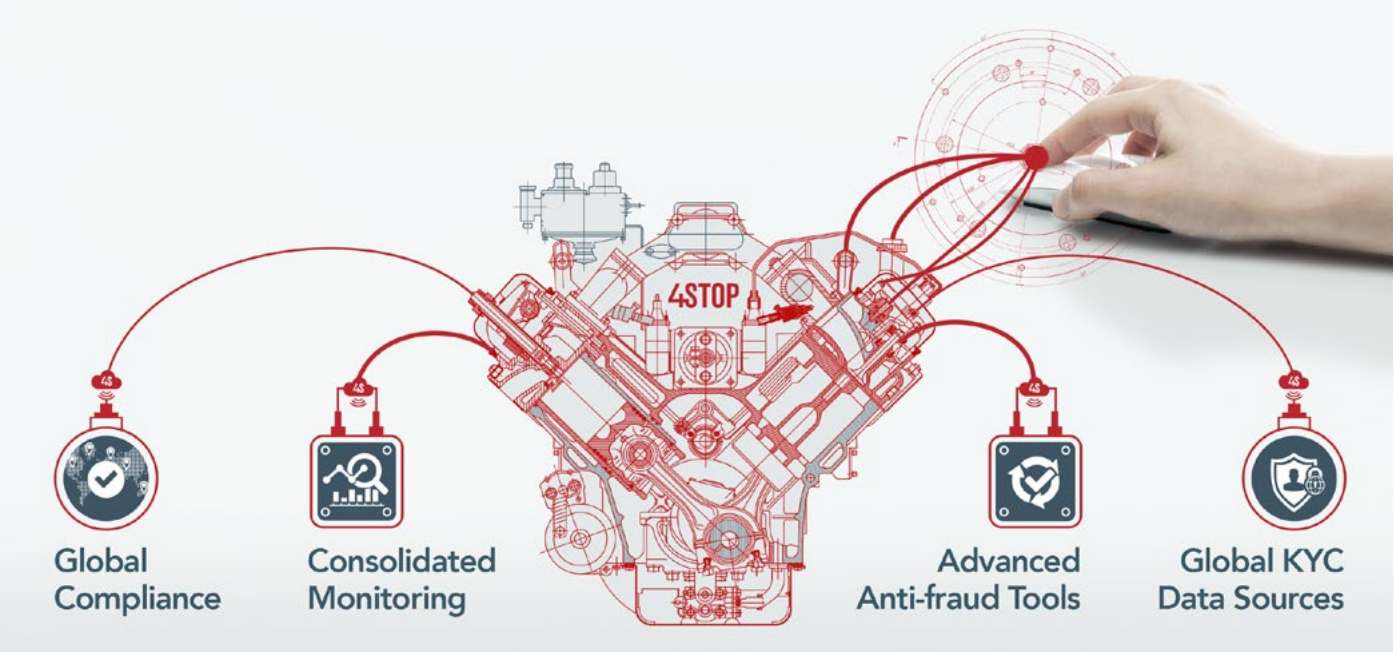
Ingo: A4Stop combines all of the global data sources to provide businesses with a full future proofed solution to expand into any market they want to with confidence their risk is managed.

With our new focus on adding machine learning to our current risk management system, we will adapt to that trend through partnerships with the thought leaders in that area.

The full suite of KYC, risk management and anti-fraud is something we see as a key differentiator as one integration covers it all for businesses needs today and their tomorrow.

PCM: What were some of your biggest challenges for launching this business?

Ingo: The market was not ready at the time we were looking to expand globally. The entry level barriers and sales cycles were still high and long because businesses like marketplaces, financial institutions and large players in various verticals did



not feel the regulatory pressure to implement global KYC and Compliance procedures and data sources.
With the PSD2, AMLD4 this perception and recognition for ensuring required KYC and compliance processes are implemented has changed drastically.

PCM: Tell us about your expansion plans and how you go about choosing the next region to expand into.

Ingo: We have seen excellent traction in the Asian, Russian, LATAM and Australian market where 4Stop is already working with the premium data sources. Our platform is consistently updated on a bi-weekly or monthly basis with the expansion of adding 2-3 data sources in each update. Additionally, we have continued roadmap development to further expand leading-edge feature-rich technology.

PCM: What are the 3 things you want people to know about your platform?

1. One Integration – Global Compliance and Single View of Risk
2. Future Proof your Business
3. IT Independence – Focus on your core business

4STOP

Payments & Cards Network

Driving Innovation through knowledge

WE WOULD LIKE TO HEAR FROM YOU

We value your feedback and ideas!
If you'd like to discuss a specific topic, don't hesitate to contact us.

Get in touch today and maybe you will be featured in the next edition:

Amsterdam Office
Herengracht 576
1017 CJ
Amsterdam
The Netherlands

Email: info@paymentsandcardsnetwork.com
Tel: +31 20 3030 257
Fax: +31 20 8208 295

Follow us now and stay up-to-date with the latest happenings in the payments world!