Vol 3. Issue 2 | February 2017

PCM

YOUR GATEWAY TO THE WORLD OF PAYMENTS

Fraudsterland

Are you doing enough?

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

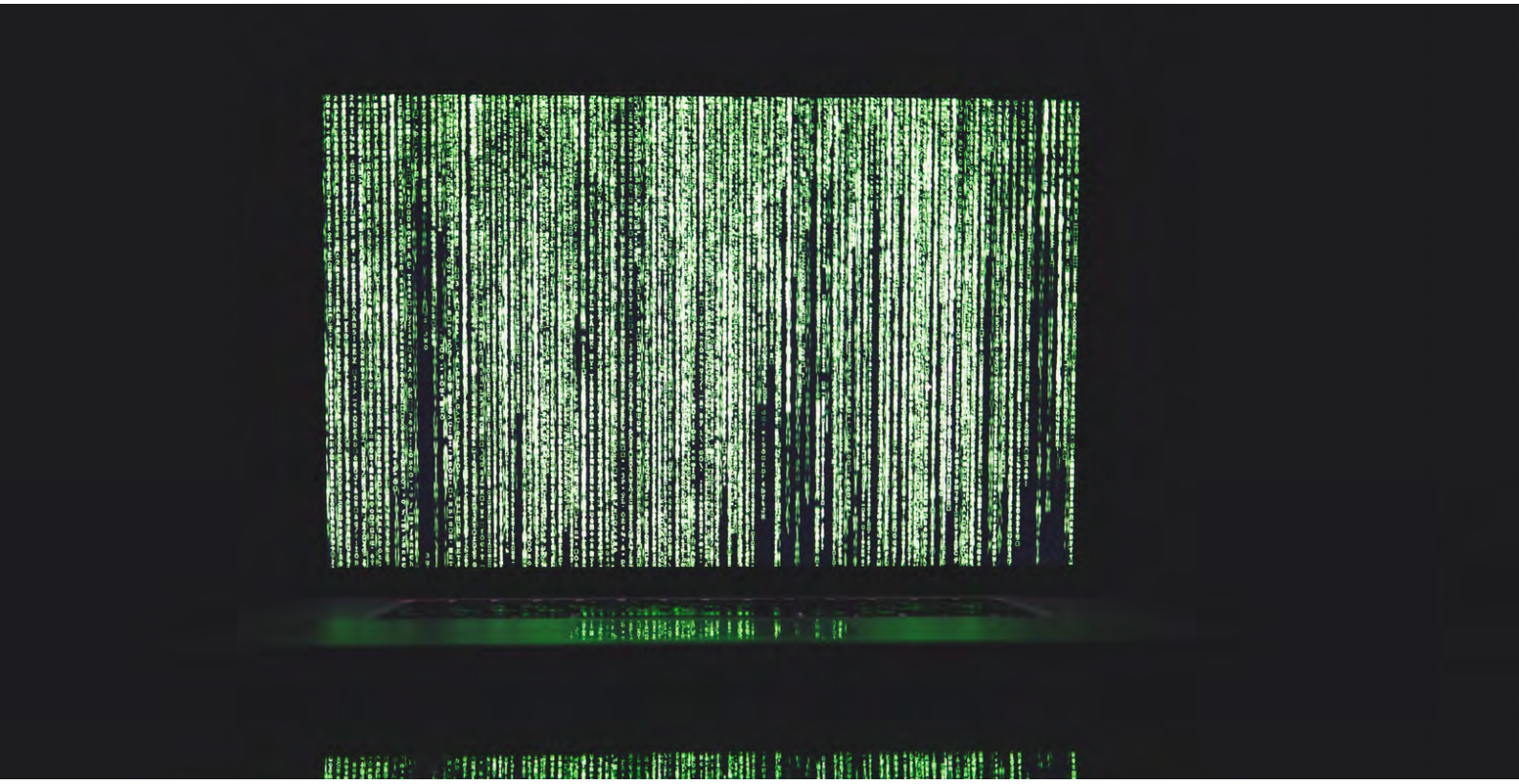
Contents

STORIES

THANKS TO OUR PARTNERS

MRC Building Better Commerce
Fraud & Payments Professionals

mondato



Trust the Machines – Let Them Help You Fight Fraud

by Roberto Valerio

Anyone who's seen The Terminator, The Matrix or more recently Ex Machina could be forgiven for thinking that the machines will inevitably turn on us. The reality away from the big screens is that artificial intelligence and machine learning is all around us and is benefiting our lives in more ways than we had perhaps appreciated.

For example, Spotify is using machine learning to evaluate user preferences and suggest increasingly accurate new music recommendations, while car manufacturers are using it to create the first road-safe driverless cars. Already we're depending on the power of machine learning for important personal issues too; medically it's being used to research disabilities and prevent avoidable hospitalisations, while in an increasingly threatening global fraud landscape, it helps protect us every day.

Fraud threats are evolving constantly as criminals devise more inventive ways of bringing down online businesses. Last year, Risk Ident conducted a survey which found that online merchants had a rather long cycle when it came to adjusting

their fraud prevention rules: 42% change them once a quarter, 26% once every six months and 22% only readjust them once every year. This is dangerous, as fraudsters don't sit still or update their tactics every quarter or year; they evolve their methods constantly, probing for weaknesses to exploit.

Fraud prevention should be able to intelligently evolve to meet these changeable threats as they arise. In the near future we can expect to face the following challenges:

Data Breaches

In 2016, Yahoo fell victim to one of the most devastating breaches we've ever seen, reportedly leaking data from more than 1 billion user accounts, while UK telecoms company TalkTalk was fined a record amount by the authorities for allegedly failing to apply "the most basic cyber security measures" for 150,000 customers. A recent Office for National Statistics (ONS) survey estimated that the UK saw 3.6 million cases of fraud and 2 million computer misuse offences last year, making fraud "now the most commonly experienced offence."
This trend will only continue in 2017, where hacking will target private user information, including names, email addresses, telephone numbers, dates of birth, passwords and security question answers. Collectively we need to identify such threats early and minimise any potential damage.

Snooping on social media

Social media leaves our personal information vulnerable to fraudsters who use Google, Facebook, LinkedIn and Twitter as research facilities. The number of identity theft victims rose by 57% between 2015-2016, according to non-profit organisation Cifas, who attributes this sharp rise to information made public on social sites. It has never been so easy to piece together information on a specific person, and sometimes no technological expertise is needed: fraudsters simply take advantage of people sharing too many details publicly, which should be kept private. Spreading awareness about the dangers of over-sharing will help cut the levels of damage fraudsters can cause.

Account takeovers

Every internet user has a lot of different online accounts. Instead of using unique passwords for every service – as experts suggest – most of us take the easier route and re-use a few favourites. But the fraudsters are aware of this weakness and are using it to their advantage. For example: shopping on the black market in the dark corners of the web, fraudsters can buy usernames and passwords and use them to try multiple other accounts online. We expect fraudsters to attempt even more in 2017.

Booming bots attacks

Disruptive smart software can generate spam, vandalise information on Wikipedia or try to influence opinions on social media. But bots are helping fraudsters as well. For example, when it comes to ticketing, bots are often able to order tickets faster than real customers. The number of bots, and the level of their intelligence, will continue to increase in 2017, so expect the ticket black market, among others, to grow.

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.

Mobile Shopping

The number of Europeans regularly using a mobile device for payments tripled from 2015 to 2016 (18% to 54%), according to Visa. Through a mixture of contactless, online and in-app payments, more of us are using mobile devices to complete transactions. However, fraudsters are using these new channels to exploit weaknesses. Often they will use multiple portable devices, alongside other masking techniques, in attempts to avoid triggering fraud alerts.

Man and machine – a perfect team

Using data science and machine learning, online merchants can create intelligent algorithms capable of detecting connections between individual transactions as well as unidentified fraud scenarios.

While fraudsters seek to conceal their locations, mask their identities and trade payment card details or other personal information online, machine learning technology is able to find patterns, calculate risks and halt their activities – in real-time.

Fraud managers are indispensable in this process. A human being with years of experience fighting fraud can never be replaced by a machine, but a combination of the two entities can produce fantastically accurate results. Domain experts know their fraud problems best but they need scalable software to help. By constantly feeding their knowledge on the context and causes of fraud into the machine, the system can evolve continually. Fraud managers can therefore scale their fraud protection system by teaching the machines to help monitor for illegal activity.

This new strategy is now being taken up by merchants across the world and will become ever more critical in helping turn the tide of online fraud. Once the machines have been intelligently taught, they can become a scalable, accurate and consistent weapon to help us terminate fraud threats before they unleash chaos across the online world. The machines are not turning on us – they can make our lives better and help merchants take on fraudsters.

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

SHOPTALK

MARCH 19-22, 2017 • ARIA, LAS VEGAS

GET YOUR TICKET | SHOPTALK

5,000+ ATTENDEES • **500+** CEOs • **300+** SPEAKERS

HEAR FROM THE INDUSTRY'S BEST LINEUP OF RETAIL & ECOMMERCE EXECUTIVES

INCLUDING

amazon

PETER FARICY
VP, Amazon Marketplace

STEPHENIE LANDRY
VP, Amazon Prime Now

GET YOUR TICKET NOW
SHOPTALK.COM

USE CODE: PAYCN150
& SAVE $150

How to commit fraud – Part 1

by Edoardo Fiorentini

Of course, I'm not going to tell you how exactly to look for tools and tips on how to commit (or prevent) fraud. But trust me, there are tons of websites and material for both those who want to commit and prevent fraud. In both the case of wanting to perpetrate or prevent fraud, the initial questions are the same:

- Where can I get more profit from circumventing a system?
- What products would I steal and how?
- Do I pay with credit card or do you offer other (questionable) payment methods?

And:

- Where can I get more profit from circumventing a system?
- What products would I steal and how?
- How do I bypass the payment part?

Bottom line, the question remains for both those who wish to prevent and commit fraud: Have you googled it?

So, let's begin with the point of view of a fraudulent guy. Let's call him Mark. Mark has been laid off his IT position after some budget cuts. He knows his way around Windows and network configuration. Mark is also savvy around forums and communities. The anonymity he gets behind his keyboard

feeds his arrogance and the feeling that the world owes him everything.

How to commit fraud? Identify your prey. Who is the victim of your plan? Perhaps an old retired man that you plan to use as a mule? Or are you thinking about stealing the identity of someone in a coma and requesting loans in his name?
I hope you see where I'm going here. Fraud seems a harmless act when you don't consider the victim. But you have to. He is the one you want to steal from, right? So... Sun Tzu's quote "Know your enemy" should ring a bell.

"But I'll steal from big corporations and that's like not stealing because they make millions".

It's not for me to judge if these corporations truly deserve their millions, because they actually produce richness. But anyhow, contributing to their losses may impactbudget cuts that will hurt their lower level employees and could lead to unemployment.

However, like everything in life, (what does this mean?)

All ecommerce companies deal in some way with fighting fraud. Either directly, by employing bright workers and developing brilliant tools, or indirectly as a cost when redirecting the service to an external provider. Either way, anyone working in this sector, will tell you that minimal losses are not only acceptable, but actually put the whole department cost in question. Some have even admitted, after a few, that they might not mind a bit of fraud, to justify the budget needs.

So, since you want to avoid being seen and drawing attention to your fraud, you want to stay between certain parameters of "acceptable risk". If you plan to steal a watch, you may be more successful getting a plastic one rather than a gold one. Of course the reward is bigger on the higher value item, but you don't want to be a single hit guy remember? You want to dedicate to commit fraud in a professional manner. Guess what, you can't do it properly from behind bars, can't you?
On the prevention side of the coin, life goes on in quite a similar pattern. You can't reject orders based on small suspicions. Nor can you afford the cost of manually reviewing all orders (Imagine life if this was the magical formula to prevent fraud!). You need to find the balance to reach an acceptable risk rate compared to the resources employed in the operation. Please, read the above paragraph addressed to our fraudster. He is not so stupid as to go for the most expensive item you have in the store. He knows you will have some value triggered rules in your system and he will circumnavigate them. And believe me, the fraudster who doesn't know your values will test your system with a few orders to understand your velocity rules and your value rules. Once he understands the schema, there will be a series of chargebacks that you will categorize as "unavoidable at that time". However, since you will have questions about your operation, you will still want to keep that healthy balance between acceptance rate and chargeback rate.

I was once hit by a fraudster we called the "Indonesian guy". We received solely fraudulent looking orders—he wasn't even trying to get the orders through.. And I couldn't t sleep at night thinking that this guy was testing my system, my rules etc.
Luckily for me, he was doing referral fraud and thanks to the connections I had at Paypal, I was able to push this guy somewhere else to do something similar—but elsewhere.
That's what we do in risk prevention, don't we? We push

Edoardo Fiorentini

Risk Management Expert

Edoardo "Edo" Fiorentini has worked as risk manager in numerous e-commerce businesses. He also is co-chair of the Fraud Committee and European Advisory Board of directors of the MRC (Merchant Risk Council). This gentleman describes himself to be a passionate risk professional with years of experience with CNP transactions. Edo has been fully dedicated into achieving and maintaining the difficult balance between fraud management and conversions in e-commerce.

fraudsters somewhere else. Let them steal money from someone else. Still, a good person would alert the neighbours if there is a thief roaming around the neighbourhood. But not so in ecommerce, let's just push them away to someone who doesn't have sophisticated fraud prevention systems.

And you think that being too good at preventing fraud is cool? It may be true that if you kill fraud, your budget will decrease. Ask a fireman. Once there are no more fires and there is no immediate threat , how easy will it be to receive additional budget? No, I'm not suggesting you to let a big fraudster hit your company to be able to receive a bigger budget to "fix" the problem. That will get you fired in the process. In that case,, your former company will now spend more budget to "fix" the problem, without you.

Stay tuned for more!

Risk & Fraud Trends to Watch for in 2017

by Stephen Ufford

Hacking email accounts to influence the US election. Millions of passwords stolen in one fell swoop. The use of stolen card data in card-not-present (CNP) situations surging 40% in one year. You don't need to look far to see incidents of risk or fraud - and the problem seems to be getting worse.

What can you do as a payments industry expert to watch out for new threats and protect your business from fraudsters and other attacks? Of course, the issue is multi-pronged, as there are numerous types of threats to guard against and, numerous techniques to assess. Let's take a look at some of the biggest challenges in 2017 and possible solutions.

Increasing Globalization

One of the biggest benefits of e-Commerce is the ability to sell to almost anywhere and anytime, regardless of physical location. Thus, selling online requires effectively dealing with the vagrancies of international payments, different payment providers, modes of payment, verification method, common practices, and regulations. One example, requiring AVS on order validation is an unnecessary step for global commerce, yet 70% of retailers rely on it.

It's not enough to identify a market opportunity, set up and sell; situations change and your standards must be kept up to date. In Europe, the new General Data Protection Regulation (GDPR) is coming into effect in 2018 and requires reporting of any data breach within 72 hours, among numerous other requirements. Businesses need to start preparing now to ensure that they are in compliance.

Another global threat that is especially concerning is cyber-warfare. The escalation from information gathering to cyber-attacks portends an era where businesses are at threat by sophisticated, nation-state backed groups. The more critical a company is, the more likely it will be a target. Businesses need to report breaches as soon as possible and work with industry groups to ensure that they are using best practices.

Increasing Sophistication

Unfortunately, as the cyber-attack groups demonstrate, the criminals are getting more sophisticated. In many cases you're not up against just a lone hacker, but rather, organized criminal groups that have deep resources at their disposal.

To counter this, you need to implement more sophisticated fraud prevention techniques. Analyze more data for patterns that indicate fraud; a surge in particular browser types or particular types of purchases or other discrepancies warrant further attention. Cross-checking purchases to previous orders can point out problematic customers, or on the contrary, indicate a good client. Implement best practices, such as tokenization, encryption, identity verification and risk engines to better detect and prevent fraud.

Increasing Mobile

It seems no account of any payment industry trend can be without a mention of mobile. Mobile commerce is exploding, accounting for 61% of total e-Commerce traffic. While many are using mobile for discovery only and use a desktop for actual orders, mobile revenue is also growing. While a perception of risk still persists, mobile purchases are actually 45% safer than desktop orders, according to Riskified data. The largest risk in mobile is losing the sale. Abandoned carts are a major issue; for maximum results, simplify complicated ordering processes, enable easy mobile payment options such as; Google Wallet, Apple Pay, and PayPal; and take advantage of unique mobile data (carrier info, GPS, and social media).

Increasing Intelligence

The world is getting faster and mere mortals have a tough time keeping up. Lucky for us, there is a whole new range of tools that will increase our capabilities, simplify our processes and make us look like heroes to our bosses. However, businesses taking no action and opting to take a 'wait and see' approach risk falling behind in technology, new processes and capabilities. The speed of innovation will not be kind to dawdlers, as the gaps created now will be hard to overcome.

Machine learning and other Artificial Intelligence (AI) techniques offer the potential to analyze more transactions, on a deeper level than a team of fraud experts. This is not to say that AI can replace your fraud team, but rather, it allows them to focus on more difficult cases where creativity and ingenuity come into play.

Working together, fraud prevention teams and smart technology offers a way to limit risk while still taking advantage of growth opportunities. As the potential for fraud and risks grows, smart payment experts need to up their technology game; the tools are there, the question is will you use them?

Stephen Ufford

CEO & Founder, Trulioo

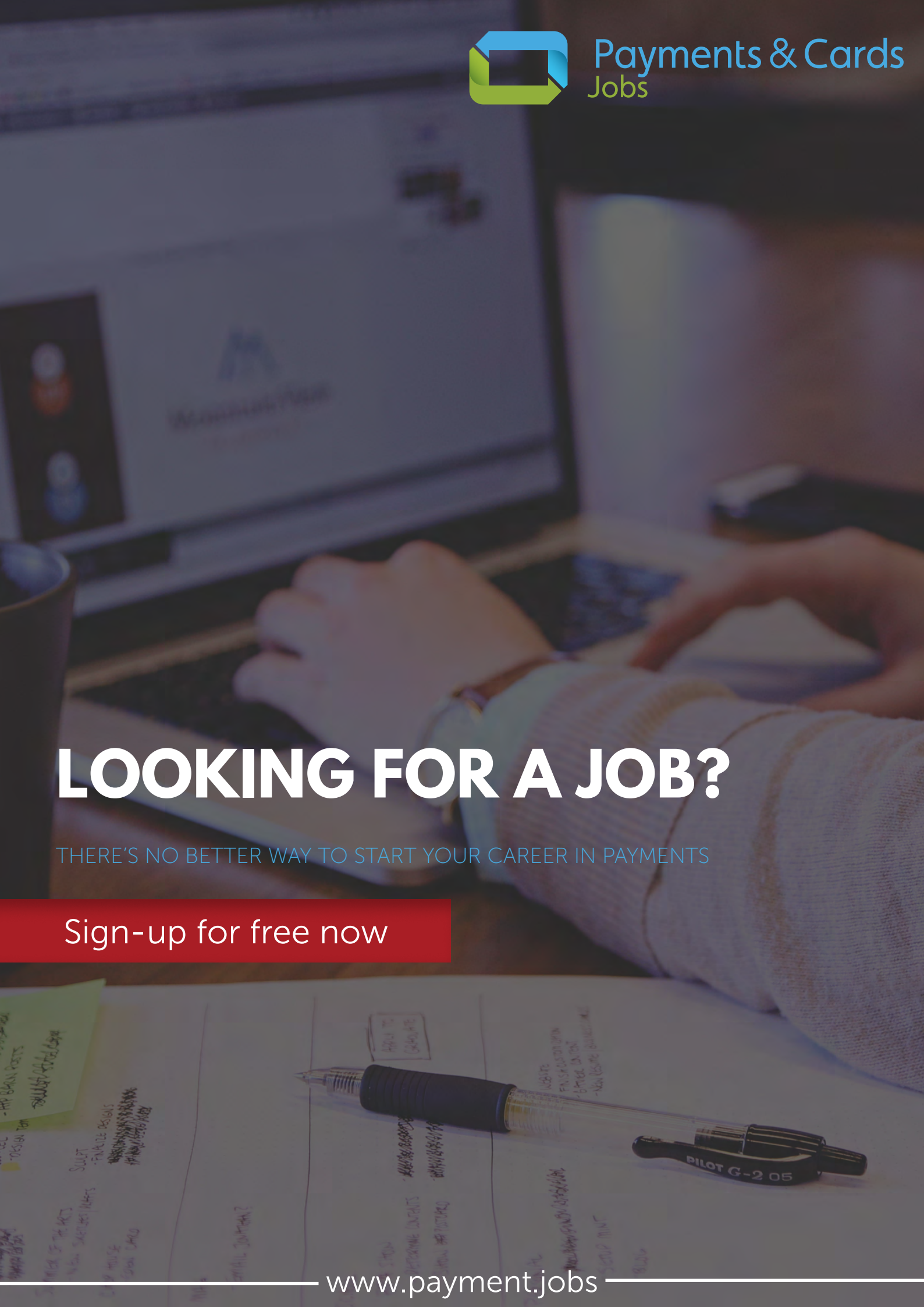
Stephen has founded several consumer data focused startups over the last decade while working in the role as CEO. In 2011, the identity veteran started his most recent startup, Trulioo, a global identity verification company focused on building a framework of trust online, implementing best privacy practices, and advancing financial inclusion.

Trulioo

The Identity Bureau

Trulioo

Trulioo is a global ID verification company that provides advanced analytics from traditional and cyber data sources to instantly verify identities online. Trulioo's bank-grade identity verification API enables businesses to perform frictionless identity verification for 4 billion people in over 60 countries via more than 200 data sources - the widest coverage in the market. GlobalGateway helps businesses comply with Anti-Money Laundering (AML) and Know Your Customer (KYC) identity verification needs, and provides a reliable and trustworthy way for businesses to evaluate new and existing users through one, single portal or API.


Payments & Cards
Jobs
LOOKING FOR A JOB?
THERE'S NO BETTER WAY TO START YOUR CAREER IN PAYMENTS
Sign-up for free now
PILOT G-2 05
www.payment.jobs

Chargeback & Friendly Fraud

Monica Eaton-Cardone is the COO of Chargebacks911. She is an internationally-renowned thought leader and expert on payment processing, eCommerce sustainability, and risk relatively. She was recently named Executive of the Year and Innovator of the Year through the American Business Awards. Connect with Monica on LinkedIn or Twitter.

For many merchants, chargebacks are a hidden threat that slowly siphon revenue until loss is an unmitigated liability. But what are chargebacks? How can merchants gauge their risk? And what can be done to stop the needless revenue loss?

PCM: What are chargebacks and who is afflicted by them?

Monica: A chargeback is a forced credit or debit card refund. A cardholder's bank will forcibly remove funds from the merchant's account and return them to the cardholder.

Valid chargebacks can be requested in cases of fraud. There are two types of fraud that warrant a chargeback.

1. **Criminal fraud:** A criminal made an unauthorised transaction without the cardholder's consent.
2. **Merchant fraud:** The merchant didn't fulfil obligations. Examples might include: failing to ship merchandise, not acknowledging customer queries, refusing to provide refunds for qualified transactions, etc.

Other situations might prompt an illegitimate chargeback, known in the eCommerce environment as friendly fraud. Friendly fraud chargebacks are usually divided into two categories:

1. **Accidental friendly fraud:** The cardholder didn't realise the chargeback wasn't appropriate or was predicated on illegitimate reasoning. For example, the cardholder didn't recognise the business's name on the bank statement and assumed it was an unauthorised purchase.
2. **Intentional friendly fraud:** The cardholder sets out to get something for free (cyber shoplifting) or opts for the most convenient resolution. For example, the cardholder might suffer from buyer's remorse and claim the product wasn't delivered—when it actually was.

It is important to note that valid chargebacks are a powerful and necessary consumer protection mechanism, however, the rise of friendly fraud shows consumers have learned to exploit loopholes in the archaic chargeback process. Devised in the pre-internet era, the chargeback process is not designed to provide an equitable resolution for eCommerce disputes.

However, because of friendly fraud, merchants are suffering unjustified revenue loss, and consumers are experiencing consequences of their own doing. Friendly fraud causes merchants to lose the merchandise and revenue, experience increased fines and penalties, and ultimately, jeopardise payment processing capabilities. Meanwhile, consumers will start paying more for the same goods and services because merchants must compensate for the additional losses and costs. And, if the bank suspects the cardholder is soliciting illegitimate chargebacks, the bank account could be closed and the credit score damaged.

Merchants loose roughly €37 billion to friendly fraud each year, and rates increase between 41-55% annually, depending on the industry and geographic location.

PCM: Why does friendly fraud continue unchecked?

Monica: There are several reasons why

the friendly fraud epidemic continues. And, until these issues are resolved, merchants won't see a reprieve.

An Outdated & Non-Compliant Process

The chargeback process was created in a pre-internet era and has experienced very few adaptations to accommodate modern transactions. Changes that have been made to card scheme regulations (Visa, Mastercard, etc.) take advantage of technologies to streamline processes, not necessarily to identify and rectify shortcomings.

In conjunction with the static regulations that haven't evolved in tandem with emerging eCommerce fraud opportunities, the chargeback process lacks consistently-applied standards. The lack of transparency regarding how and if regulations are enforced makes it difficult to achieve effective and sustainable remediation.

Learned Consumer Behaviour

Experts claim we live in the "Age of the Consumer," with instant gratification being the dominate characteristic. Consumers expect prompt results in everything they do, including transaction dispute resolution.

A survey of customers who had filed an illegitimate chargeback revealed 81% had acted out of convenience—it was easier to call the bank than the merchant.

Because friendly fraud is increasing at such a rapid pace, merchants and issuers are ill equipped to handle the influx. Issuing banks don't execute the needed due diligence to detect friendly fraud, and merchants don't challenge illegitimate transaction disputes. As a result, consumers perceive chargebacks as a no-hassle alternative, void of consequences.

Management Challenges

Card schemes have issued "reason codes" to help banks explain why a given transaction has been disputed. However, friendly fraud can be disguised with virtually any reason code. This makes it challenging for merchants to differentiate between valid and invalid chargebacks.

As a result, merchants lose a significant portion of revenue—as much as 87% of all chargebacks are illegitimate—that could be recovered if they were able to conclusively identify friendly fraud.

And, the vicious cycle continues. Merchants don't challenge friendly fraud, so consumers don't perceive drawbacks to their faulty behaviour and issuers aren't compelled to comply with industry regulations.

1-10%
Criminal Fraud

Criminal fraud stems from identity theft, stolen payment cards, and cyber criminals. Typically, chargebacks from criminal fraud represent only a fraction of 1% of merchant chargeback cases.

60-80%
Friendly Fraud

Cyber shoplifting and friendly fraud make up the vast majority of chargebacks.

20-40%
Merchant Error

Surprisingly, errors in merchant setup, transaction data, and order processing account for more than 20% of merchant chargebacks.

PCM: Is there anything that can be done about friendly fraud? Or is it just a cost of doing business?

On the surface, it seems like there isn't anything that can be done about friendly fraud, and many merchants do accept it as a cost of doing business. But at Chargebacks911, we've made an important discovery.

All that's needed to manage friendly fraud is an understanding of transaction disputes by source. Every single chargeback can be traced back to one of three things: criminal fraud, merchant error, or friendly fraud.

If merchants are able to identify the source of a chargeback, they can create effective prevention and dispute tactics. Otherwise, merchants are simply treating symptoms if they are not solving problems at their source.

Chargebacks911 has created a unique technology, Intelligent Source Detection, which identifies chargeback triggers. That technology, combined with our expert management strategies, helps merchants reduce criminal fraud, eliminate merchant error, and then fight everything that's left—which is friendly fraud.

The concept seems simple, and for those who take advantage of our technology and expertise, it is. But for those merchants who are determined to mitigate chargebacks on their own, it's best to manage based on the card schemes' reason codes to avoid disputing legitimate chargebacks and damaging client retention.

And, since representment opportunities will be limited without ISD technology, it's best for merchants to try preventing friendly fraud.

- Use easy-to-recognise billing descriptors.
- Provide exemplary customer service (answer the phone when it rings, reply to emails, respond on social media, etc.).
- Consider a user-friendly return policy—the less restrictive, the better.
- Use delivery confirmation, at least for big-ticket items.
- Use additional identification verification methods, like texting an authorization code or verifying with social media.
- Fully disclose the use of Dynamic Currency Conversion.
- Request the card security code.
- Promptly issue refunds for qualified purchases.

PCM: Why don't traditional fraud detection tools work for friendly fraud?

Monica: Some fraud detection tools—such as card security codes, 3D Secure, and Address Verification Service—will help build a compelling case against friendly fraud, but won't help prevent it. Fraud filters won't help either. Fraud filters are based on machine learning: they analyse characteristics of confirmed criminal fraud to very successfully prevent future instances. However, since friendly fraud results from authorised transactions conducted by loyal customers, the defining characteristics of fraud won't be applicable.

Trying to use fraud filters to detect illegitimate chargeback potential will be a costly mistake. Tightening fraud filter rules will simply result in additional false positives, needlessly declining good sales. Also, it will damage customer loyalty and brand reputation.

If you think friendly fraud has, or will, become a liability and would like help creating an effective mitigation plan, seek professional assistance. Any of the chargeback experts at my own company, Chargebacks911, would be happy to help. Get an expert opinion on what does and doesn't work with your current strategy, as well as ideas on how to enhance your efforts. It is best to take a proactive stance, rather than function in reactive mode once chargeback rates escalate.

PCM: How do you determine if chargeback rates are "dangerous?" When is it time to get help?

Monica: Chargeback management is an essential task for any eCommerce merchant. While it might be tempting to disregard chargebacks as a nuisance or minor profit drain, they actually impact the business's longevity.

If the chargeback-to-transaction ratio exceeds 1%, payment processors are forced to take remedial action against merchants. In an effort to mitigate their own risk, processors will likely start penalising a merchant long before the 1% threshold is breached.

Once payment processing capabilities are lost, the business's sustainability has forever been impacted. Obtaining new merchant agreements will be time consuming, expensive, and difficult. Therefore, it is advisable for merchants to take a proactive approach to chargeback mitigation before risk becomes an unchecked liability.

Merchants should watch for the following warning signs, as these indicate immediate action is needed:

- Chargeback-to-transaction ratio above 0.5% -- Card schemes will issue warnings once ratios hit 0.75% and enter merchants into a monitoring program at 1%.
- Chargeback value-to-transaction value ratio above 0.5% -- Some processors are only watching the chargeback value, not the count, because merchants are running many low-value transactions.
- Number of chargebacks categorized as fraud increases by 20% or more in a 14-day period – Card schemes will penalise merchants for this and enrol them in monitoring programs.
- Revenue holds are implemented – If acquirers sense risk is escalating, they'll implement revenue holds as a form of insurance to protect their own assets.
- Acquirer has requested a mitigation plan – Acquirers will need to determine if elevated risk levels are temporary and can be remediated or if they are permanent and uncontrollable.
- Enrolment in a chargeback or fraud monitoring program – Merchants must lower chargeback and fraud rates—and keep them low—within a predetermined time period or processing rights will be revoked.

While these general warning signs can help you gauge risk, a personal review of your business's unique situation would be best. There might be other, hidden, indicators of trouble, as well as simple changes that would make a significant impact and greatly reduce risk. Again, I'd be happy to help—asking for assistance is the first step toward creating change.

Chargebacks911

Chargebacks911, a Global Risk Technologies company, provides comprehensive chargeback management services with guaranteed results. Dynamic, scalable solutions are customised for 26 different industries with the flexibility to accommodate any payment method or sales tactic. Chargebacks911's 350 employees manage 200 million transactions monthly from locations in North America, Europe, and Asia.

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.

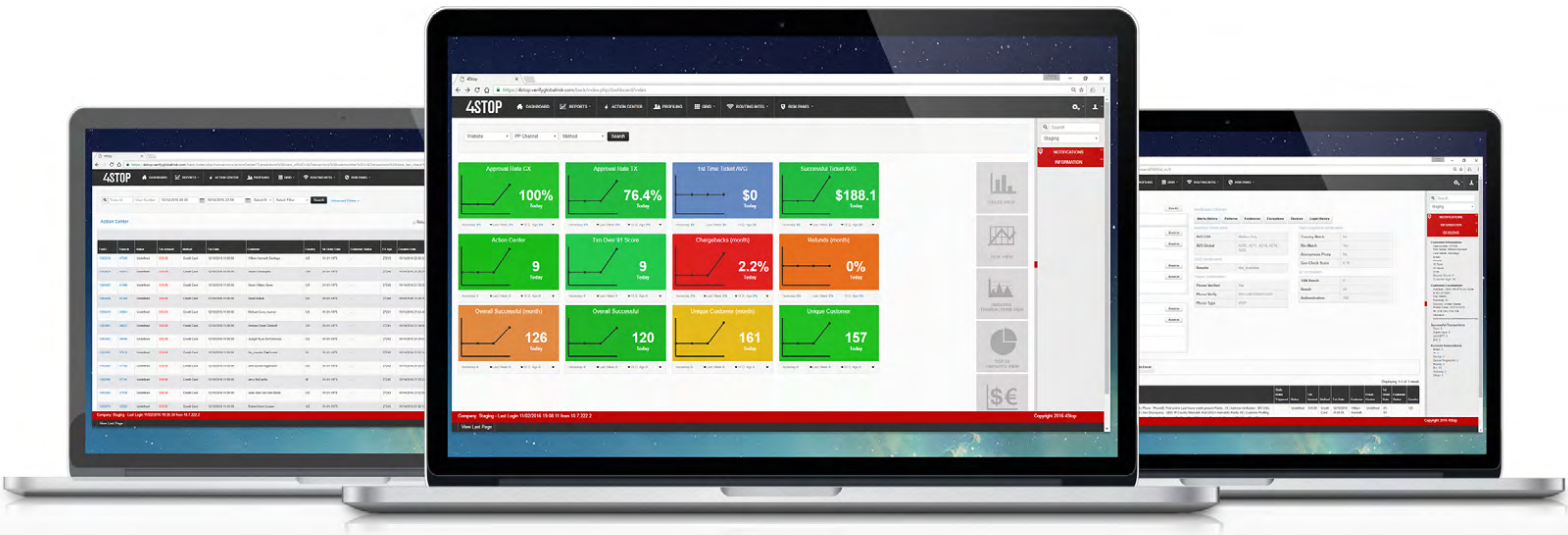
The primary obstacle in setting up a streamlined risk-based approach and a globally scalable set of data providers for compliant KYC procedures is the challenge of having to integrate various data provider at different touch points in the customer experience. Traditionally this has been solved by various 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?

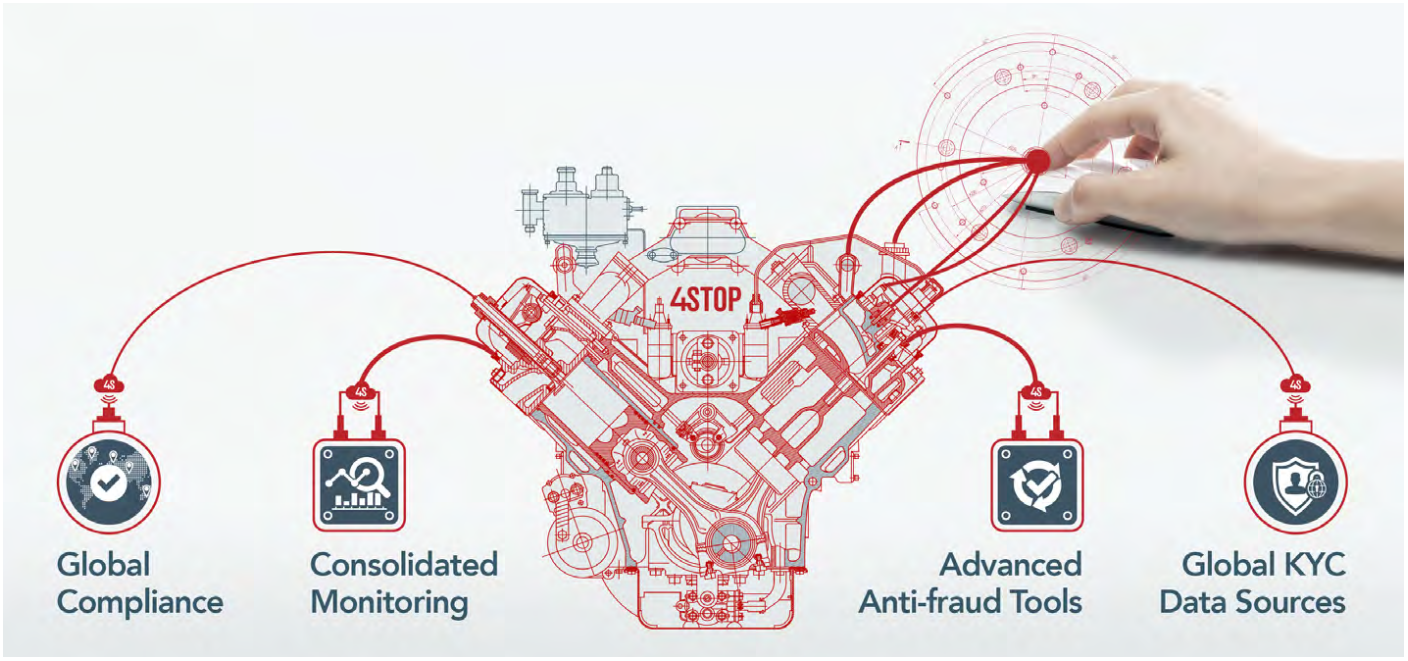
Ingo: A4Stop combines all of the global data sources to provide businesses with a full future proofed solution to expand into any market they want to with confidence their risk is managed.

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

Hot Jobs

BID MANAGER

Paris | France

SENIOR FRAUD CONSULTANT

Amsterdam | The Netherlands

REGIONAL MANAGER SALES

Frankfurt | Germany

FRAUD PREVENTION MANAGER (MID-LEVEL)

Berlin | Germany

GENERAL MANAGER EUROPE

Home-based / Hamburg | Germany

ACCOUNT MANGER - GERMAN

London | UK

(SENIOR) MANAGER PAYMENTS CONSULTANT

Frankfurt/Hamburg/ Munich/ Düsseldorf | Germany

EXPERT & SPECIALIST IN THE MARKET INFRASTRUCTURE DEVELOPMENT DIVISION

Germany

BUSINESS DEVELOPMENT MANAGER

Home-based | regular travel to Scandinavian countries

PRODUCT MARKETING DIRECTOR

London | UK

(SENIOR) MANAGEMENT CONSULTANT

Frankfurt | Germany

PAYMENT RISK MANAGER

Paris | France

These are the latest job opportunities we have on offer!
For more information please visit www.paymentsandcardsnetwork.com
or check out our international Job Board at www.payment.jobs

EVENTS

London, UK *15 % Discount:* PCN15

Mobile Shopping is your one stop shop to meet and hear from the most senior digital pioneers from top retailers. It's the only event in Europe dedicated to mobile only. Various challenges will be tackled including but not limited to; Achieving a mobile-first approach; Marking the right investments; Easing the path to purchase and much more!

FEBRUARY 8-9 2017

Berlin, Germany

MPE 2017 is one big expo with 3 parallel conferences. It offers top class networking opportunities & evening dinners; Internationally recognized MPE Awards, MPE C-Level Club , Festival of European merchant payment methods and Innovation Corner. The addressed topics span from ACH payments, Apple, Samsung, Android Pay to integrated shopping experience, NFC, from FinTech to RegTech, SmartPOS, mobile & online checkout conversion, CNP Fraud & security, IoT, biometrics, API driven innovations, local and cross border acquiring.

FEBRUARY 14-16 2017

Hong Kong, HK

Organised by Inspira and Beacon Events, the **Financial Innovations Asia Summit** will offer the market a highly focused business and industry perspective. With no hype but practicality on top of the agenda, this event will showcase real business issues and decisions required to cope with emerging technologies and changes in business operations.

FEBRUARY 14-16 2017

London, UK

IT Risk Management in the Financial Sector will provide IT risk professionals with the information on the models being used by their peers to best manage IT risk and ensure forward looking risk management methodologies, in addition to spotlighting current challenges like cyber risk and increased regulatory engagement.

FEBRUARY 20-21 2017

FINSEC
THE BANKING SECURITY SUMMIT
21-22 FEBRUARY 2017
DUBAI, UAE

Dubai, UAE

The recent wave of attacks against banks in the Middle East using highly advanced engineering techniques underlines the gravity of the situation. There is an urgent need to develop a robust security framework as traditional methods are becoming redundant. The **FinSec Summit** will bring together decision makers and solution providers to share experiences and address key challenges.

FEBRUARY
21-22
2017

Cape Town, SA

FEBRUARY
22-23
2017

The **eCommerce Africa** conference sessions will examine various aspects of development in the industry: how online and mobile retailers are capitalising on growth opportunities; how omni-channel retailers are moving into a digital space; where the consumer is driving their own experience; the realities and challenges of cross-border expansion; and overcoming fulfilment concerns and driving logistics in the real world.

eCommerce Africa

Vienna, Austria

GLC

Following the great success of our **2nd Annual Post Trade Forum** with more than a 100 participants, we are happy to invite you to our 3rd Annual Post Trade Forum, which will be held 23rd – 24th of February, 2017 in Austria Trend Hotel Savoyen Vienna, Austria. Hear more about the global regulatory landscape; EMIR, MIFID II, T2S and forecast what is next in the clearing and settlement. Listen to our expert speakers and their real life best practices in lower post trade costs.

FEBRUARY
23-24
2017

London, UK

FEBRUARY
23-24
2017

In recent times, financials have been forced to rethink traditional operating models in favour of outsourcing models that will help improve revenue and create new business opportunities. Financials are currently embracing outsourcing as a strategic extension to the business for managing core processes, but simply outsourcing all activity is not the way forward, financials must also manage and mitigate the risk arising from their vendors.

Outsourcing and Vendor Management in Financial Institutions
London, United Kingdom
23-24 February 2017
marcusevans

Barcelona, Spain

Join us in vibrant and colourful Barcelona, Spain and be among the first to hear the best in your field deliver inspiring talks about the newest industry trends and developments at **Innovation Excellence**. Gain knowledge about the latest developments within your own field and explore uncharted territory which will also prove extremely rewarding.

Palm Springs, US

eTail, launched in 1999, is the premiere multi-channel retail conference dedicated to supporting the growth of the retail industry through high-level networking and extensive thought leadership. eTail West was launched as part of the eTail Conference series to speak to the unique challenges facing retailers looking to grow their brand in the market. Download the agenda to learn more: http://bit.ly/2fXFHV6

Frankfurt, Germany

Where the Finance & Insurance World Talks Innovation: at the **Digital Finance World (DFW)** on March 01- 03, 2017 in Frankfurt. 2,5 days packed with hottest information about blockchains, bitcoins, big data and the Internet of Value – plus pre-Conf Workshops. Listen to internationally renowned digital transformation thought leaders, finance industry professionals, fintech 2.0 founders, analysts and blockchain experts.

MARCH
2-3
2017

Berlin, Germany

Risk Management is a hot topic wherever we go. After the financial crisis and credit crunch hit the world economies the importance of Credit Risk Management emerged even more. During **3rd Annual Credit Risk Management Forum** – following in the footsteps of GLC renowned Risk Management Series – the participants will hear about the latest regulations, gain insight to volatility under IFRS 9; stress testing and scenario analysis in ICAAP and Recovery plans; risk models; shadow banking; AnaCredit, and many more.

LAST MILE FULFILMENT ASIA

Singapore

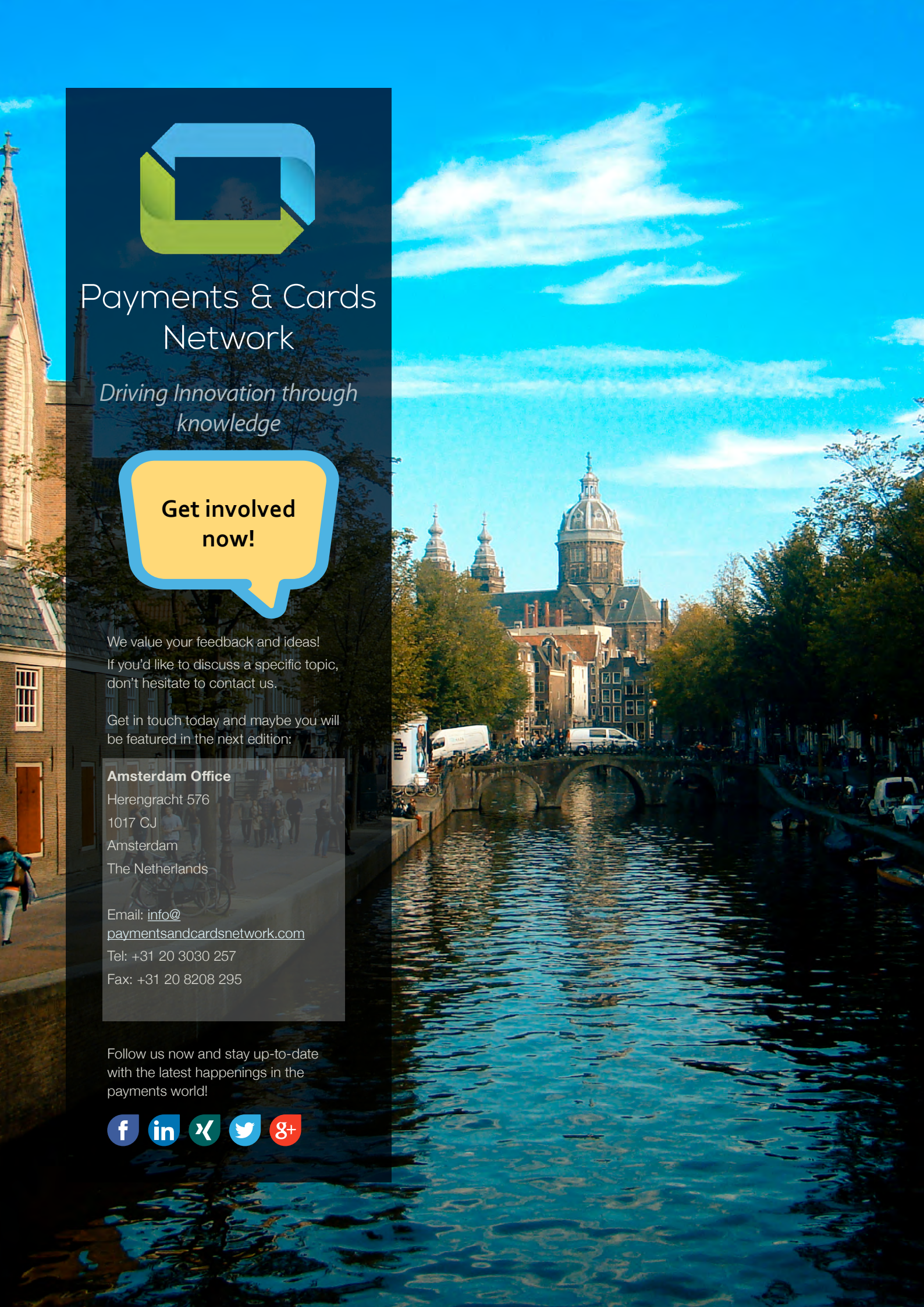
LMFAsia is the only Asian conference and exhibition to curate an ecosystem-based platform for seamless cross border last mile fulfilment in Asia. In its 3rd edition, LMFAsia 2017 will be expecting 3,500 attendees, bringing together retailers, e-commerce, postal and logistics companies from 30 countries worldwide to connect, explore business opportunities and collaborate in Asia.

MARCH
2-3
2017

APRIL
7
2017

Kampala, Uganda

Finnovation Africa 2017 will gather all stakeholders and influencers in the African FinTech value chain from the key markets across Africa and internationally. The event will seek to better align FinTech directions and initiatives in Africa with the strategic economic priorities and requirements of key countries – and provide a roadmap of how the banking and financial services industry across the continent can make even greater strides towards a positively transformed future.



Payments & Cards Network

Driving Innovation through knowledge

Get involved now!

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!