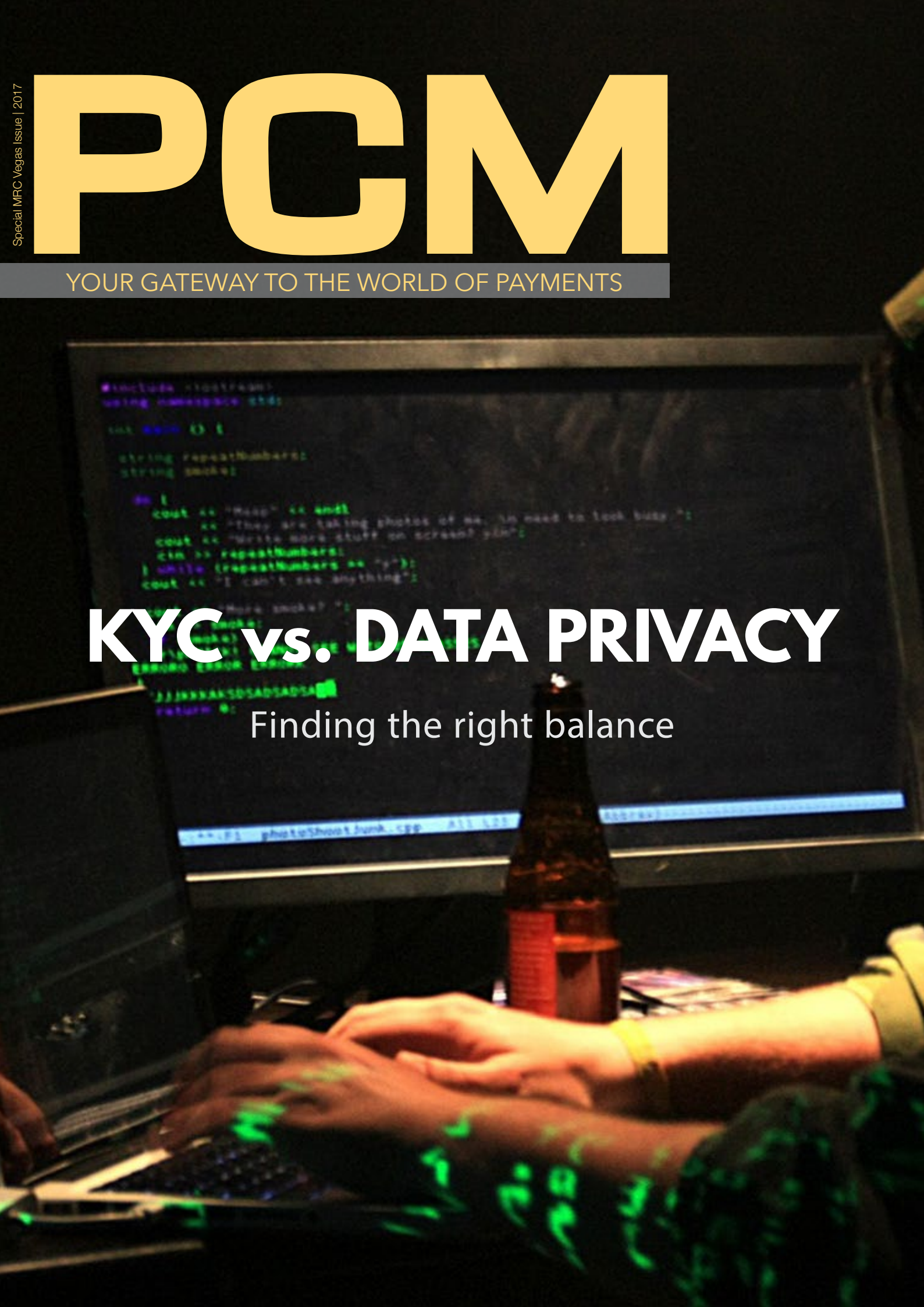
Special MRC Vegas Issue | 2017

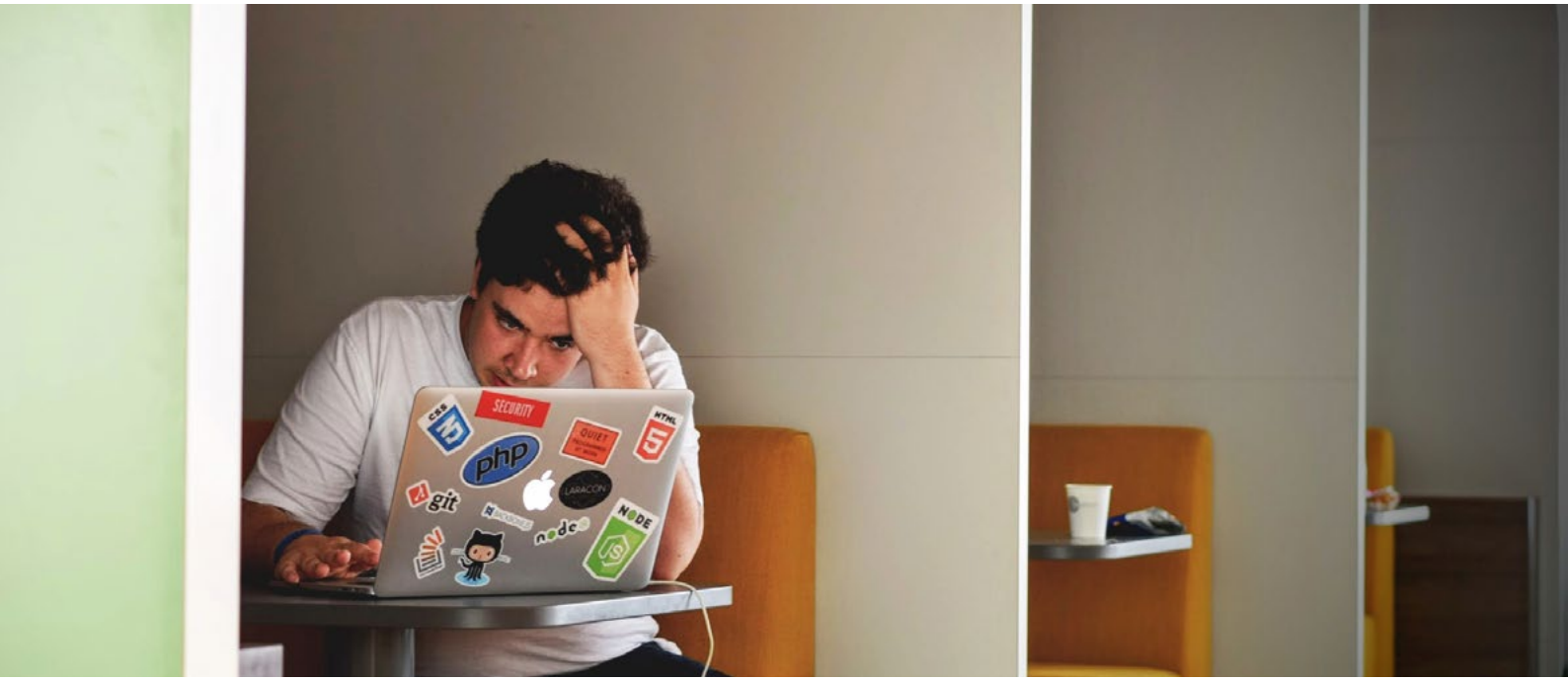
PCM

YOUR GATEWAY TO THE WORLD OF PAYMENTS



KYC vs. DATA PRIVACY

Finding the right balance



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