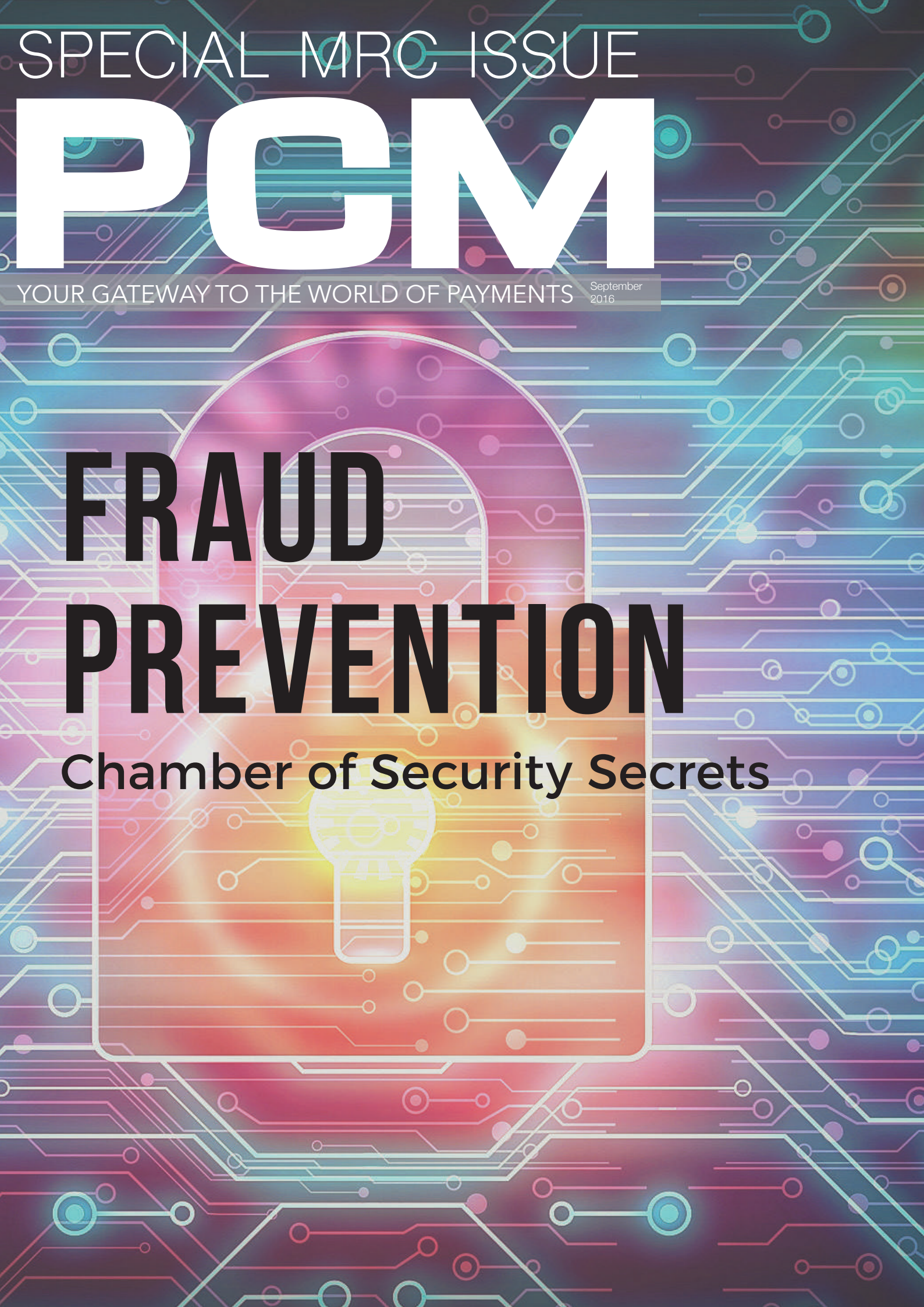
SPECIAL MRC ISSUE

PCM

YOUR GATEWAY TO THE WORLD OF PAYMENTS September 2016



FRAUD PREVENTION

Chamber of Security Secrets

email every time important account information like an address or password has been changed.

PCM: How does artificial intelligence and machine learning help to detect fraud?

RV: Fraud, especially organised fraud, is constantly changing and evolving. People who commit fraud for a living and organised criminals are adapting their tactics very quickly. Merchants are setting up rules to prevent this fraud, but the fraudsters will directly try to go around their boundaries. For example, say you have a limit for a customer shopping basket and if a purchase is below this limit, you will not look at the transaction. With this situation in mind, fraudsters will try to find out the limit and stay below the value. Another example: if you focus on specific high-risk articles, the fraudsters will try to buy unsuspicious or less expensive articles in higher quantities. So, every time you try to block them based on a concrete rule set, they will change their approach.

This is all happening within a short amount of time, which disables merchants from acting quickly enough to adapt their strategy. Machine learning takes this manual task away and learns from every fraud case that one experiences. Artificial Intelligence will adapt the existing rules to every newly registered fraud case. A manual process will always take longer to find the fraud case, evaluate it and build rules out of this, whereas the machine learning component will do this automatically. The moment you confirm a new fraud case, the machine will learn based on this specific case to adapt much quicker to the new fraud tactics from criminals. Big merchants who have thousands of transactions per day are not able to manually decide on every transaction because there are simply too many of them. The Machine learning component that Risk Ident has included in the software works on every transaction and scales to tens or hundreds of thousands of transactions. AI will help to adapt to the existing data every case you work on and every new pattern you find for the best fraud prevention.

Roberto Valerio

CEO at Risk Ident

Roberto Giorgio Valerio, CEO at Risk Ident GmbH, studied Business Administration but his programming history reaches far back. He started programming at the very young age and therefore he is very technically skilled for a business focused professional. Before Roberto started Risk Ident he was already involved in 3 other startups as a founder.

PCM: How does Risk Ident utilise the various tools in its possession to help merchants reduce risk and prevent fraud?

RV: You need three components to be good in fraud prevention. First of all, you need a large set of data - historic data and data from different sets of merchants.

The next thing you need is domain knowledge within fraud prevention, which means that you have to understand how fraudsters operate and how they try to obtain goods or services. You have to understand how every bit of information you get out of a set of transactions can help you identify fraud. Some are trivial, like the names, addresses and emails they use. But you can also take into account how their emails are structured, the time they are ordering, which kinds of products that they order etc. The way you analyse the information will help you identify fraudsters. Deriving new information out of existing data is key to use machine learning, it is called “feature extraction”. For example, if fraudsters use different emails, they will probably still use a certain pattern like johnmiller5@yahoo.com, davidmiller10@yahoo.com etc. He or she will use different emails to avoid blacklisting, but in order to memorise them easier, they will all probably have a similar structure. A different example, which might not be so obvious, are names and age correlations. There are old fashioned first names that aren’t used anymore or are probably related to an elderly person, but if a name like

this is used by a 20-year-old person, it is suspicious. It also works the other way around, there are first names that are very new and if you have an 80-year-old person using this name, it is probable that we are dealing with a fake identity. A lot of this additional information is already within your existing data, you just need to analyze it and train your fraud detection model on it.

The third component for successful fraud prevention is an advanced technology stack. At Risk Ident we built a very scalable software solution that uses different machine learning algorithms to learn from the data our customers already have. We realized that there are quite a few good analytics tools - some of them being free of charge as well - that you can use to analyze your data sets. But they are seldom ready to be used in production in real time to assess new transactions as they roll in. Scalability plays a big role if you want to evaluate and compare every single new transaction to millions of old ones within an instance. In these times of large organized fraud cases you want to make sure every new transaction is compared to its statistical twins. So you evaluate a single case with lots of transactions instead of hundreds of seemingly unrelated transactions.

PCM: What are the various ways to reduce the risk of card-not-present transaction fraud?

RV: You have to take the advantages of the online world and match it against the disadvantages that occur. The advantages are quite clear: you normally have some more information about the customer because you have an address, the person will not take the goods directly from your shop, the goods have to be sent to be delivered. You probably have the customer's buying history, which you do not always have in place when in a store. You have information about the device that is being used, so you can use device fingerprinting. You normally have other communication channels like a telephone number or email as well. In the online world, you have more information which you do not have in the offline world and you should use them to reduce the risk. If your fraud prevention tools are able to identify related online fraud transactions this can be a real advantage. No fraudster will come back dozens of times an hour to your brick-and-mortar shop cash register to try another credit card.

RISK IDENT

RISK IDENT GmbH

Risk Ident are passionate technology experts dedicated to fraud prevention using machine learning components for behavioural analytics and device fingerprinting. We help online businesses prevent fraud in real-time by identifying and stopping fraudulent transactions, monitoring millions of transactions per day.

For more information please visit **https://riskident.com/en**