

PCM

YOUR GATEWAY TO THE WORLD OF PAYMENTS

Vol 2, Issue 6
June 2016

THE BALANCING ACT

Reduce Friction &
Eliminate Fraud



'WE MAKE NEW
TECHNOLOGY
APPROACHABLE...!'

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.

Where did the idea for Risk Ident originate and what's the organization's vision?

Risk Ident started out as a project within Liquid Labs, an incubator of the Otto Group based in Hamburg, Germany. The Otto Group is second largest European online retailer. This company has an estimated 12 billion Euro annual turnover, roughly 7 billion of that is online retail. Within Liquid Labs the project team looked into different aspects where they could leverage the knowledge and data of the Otto Group. Actually Risk Ident was founded as Device Ident, which was a focused on device fingerprinting. The Otto Group's goal at that point was to use device fingerprinting for its online shops.

That's the point where I came into play because I promised

to create a device fingerprinting solution in 6 months. The good news is that our team kept that promise and delivered on time. After being approved by the Otto Group, the initial project turned into a company in March 2013 and by now has become a leading provider of fraud prevention software within the online space.

What sets you apart from other anti-fraud solution provider?

Risk Ident was able to use the knowledge of the Otto Group and its great amount of historic data to built its first fraud prevention product. With tens of millions transaction every year having the Otto Group as a domain expert (including its years of experience of how fraud looks like) is a great advantage and benefit for Risk Ident.

Even though the Risk Ident team consists out of mostly data science professionals and senior software engineers who did not have in-depth experience with fraud prevention or payments before, we were able to create some of the most technically advanced products for anti-fraud solutions on the market. The reason for that is that we might be seen as the

latest to the game but we do use the latest technology that others weren't using a couple of years ago.

As the technical landscape is undergoing continuous change and innovation, we always try to be at the vanguard of that front. So, with more than half of the Risk Ident team being either data scientists or software engineers we focus mainly on a continuously evolving product that strongly benefits from the latest technology.

Where does Risk Ident stand now and what's on the horizon for the company?

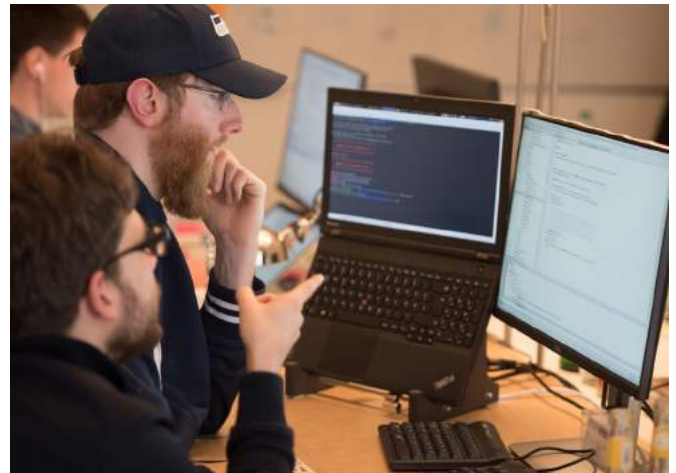
We currently have 50 clients which are mostly big enterprises. Our client group includes some of the biggest mobile network operators, big ecommerce stores (with at least 100-200 Million Euro annual turnover) Fintech companies as well as banks. I think we have a strong position in the German speaking markets and therefore have become one of the leaders on our home domain. We just started to venture into additional European market and at the beginning of next year we'll also be operating in the US.

Putting it into a startup environment perspective you commonly need three essential components to become successful. These include having a great team, building excellent products and eventually selling it to real clients. We have accomplished and gathered these vital startup elements and now it's all about how to scale up our business. Moreover, we do target only larger companies who can use our tools to enhance their fraud protection.

More importantly we realized that it doesn't matter if we sell to a big German e-commerce player, a UK based telecommunication company or an US travel portal because many fraud cases are very similar in the way fraudsters operate. One of our advantage is that the tools we built are very agnostic to the market and will also work for other markets. The only thing we have to do is to train the tools with different data. For that reasons I'd say that we have good chances to expand to new markets on a global scale.

In your experience of fraudulent transactions, what is the most common source of fraud?

When talking about online retail there are two main aspects about fraud. On the one hand, there is the single fraud cases in which commonly people with bad credit score try to obtain goods. You can usually identify them by behavioral actions like changing their name or address and they try to get one product or service. In contrast to that there is the very harmful organized fraud. These people are very professional and oftentimes even do that illegal activities for a living. What is more, they don't stop at e-commerce fraud alone, they would try to get to other people's online loans or similar personal account information. Another fact why organized fraud is considered a lot more harmful than single fraud cases is that with the increasing number of fraud cases, the risk to have full complete loss scales up. Unfortunately, the trend of organized fraud is becoming stronger right now. In conclusion organized



fraudulent activities represent the bigger problem and risk for the merchants.

Will upcoming regulations in Europe influence Risk Ident's business, and how?

Our main advantage in this regard is that our fraud prevention software can be installed on premise. That's very handy when we talk with banks for instance, as they are working with very sensitive customer information which banks won't share with third parties. And even the large e-commerce customers with the big data breaches that happened throughout the last years they were very reluctant to hand out their end customer data to a third party. When working with our software the clients can install and integrate it on premise and they can train it with its data without sending out a single customer information. That is an immense value we can offer in comparison to other anti-fraud solution provider. In that light regulations are not a major challenge for us to overcome.

How do you teach a machine to get smarter at identifying fraud?

In the light of machine learning there is one major misconception. Many people say that their machine learning component of their product is like a secret ingredient. I think that the machine learning algorithm you use is not the main advantage. There are many rather simple algorithms that can be very good, such as Random Forest, Naive Bayes or Logistic Regression. However, there are two things which are more important than the machine learning component. First of all, it's about the type of data you feed in – when feeding in low-quality data then you can only expect poor results. The other vital aspect is how to scale a machine learning system on a production level in terms of amount of data and response times. That's why Risk Ident is very transparent about our machine learning components and sometimes we even tell our customers which specific set of algorithms we use on their data because we know how hard it is to provide it on a stable productive software solution and you need to know what you put in. The machine algorithm typically will only understand numbers, so you have to get your data pre-processed also



RISK IDENT

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

known as feature extraction. Examples: An address could be converted into a geolocation, an email could be evaluated by name, domain or general structure of the email. After that you need to know how to feed it to the machine learning box and only then you can obtain good results you can work with.

To give an example for that, you can feed in an email address and the machine learning component can find other transactions with a similar email structure. Based on that I believe that the competitive advantage in our work space rather lies in how strong you are on the technology level, which contributes to your ability to build good software and ultimately making sure that the software is scalable.

What are some best practices for business owners when it comes to protecting their customer's information?

Personally I think, that one of the best practices is educating

your customers. By instructing them to not use the same password for all their different online shops and online services and reminding them to change the passwords occasionally and write them down. Simply because today it is much harder to get access to a paper note with written passwords than hacking into your laptop. To that end, it is paramount for all types of businesses to educate the end-customer about being prepared and careful about that sensitive information.

Besides, not handing out any end-customer information is of vital importance. Fraud prevention can be done in-house by using on-premise software. Every time you let a third party or service access your end-customer data you risk customer data loss. Furthermore, try to store vital customer data encrypted: Businesses should use individual hashing for passwords and to be more specific they should be using individual salts to ensure the passwords cannot easily be decrypted even after customer data was stolen.



The Risk Ident team always strives to enhance their products