Customers embrace 'intelligent friction' in fight against online fraud

Issued by Entersekt

22 Feb 2021

As the number of consumers transacting online rapidly grows in lockdown economies, bad actors have followed the money, with a spike in online fraud. Speaking at a global payments roundtable on digital fraud, Entersekt CEO, Schalk Nolte, looks at how involving the customer through 'intelligent friction' can stymie the efforts of fraudsters.

Schalk Nolte

Waiting for machines to learn

Over recent months, users flocking online due to the Covid-19 pandemic have resulted in fraudsters launching huge volleys of cybercrime attempts. Nolte describes these volume-based attacks as ‘spray and pray’ efforts and says even the new tech heroes, machine learning (ML) and artificial intelligence (AI), are battling to keep up. In fact, the World Economic Forum estimates financial crimes could cost global citizens up to $1trn dollars each year.

“Things are more focused now. It becomes a numbers game. If you have double the amount of users transacting online, even if you get just a two percent return on your emails, that’s a good rate for any fraudster. What we are seeing now just boils down to new use cases based on the same methodology,” he says.

The obvious response to the increase in fraud attempts and especially some for the more sophisticated attempts, is to throw more technology at the problem. Nolte, however, says banks and other organisations are missing a trick if they think they can just rely on new tech like ML and AI.

“The problem with so many new users is that you have nothing to compare their behaviour against. No matter how good your ML or AI is, it’s all about relying on user behaviour to predict actions. This ratchets up the number of false positives. If consumers use their credit card online for the first time, for example, and it gets declined because of a false positive result from the fraud engine, they will be far less likely to try to shop online again with that card (or at all). Machines need to experience fraud before they can learn from that fraud - its a reactive process,” explains Nolte.

Customers know best

For this reason, Nolte says getting the customer involved in the process puts boots on the ground to fight fraud and they are the most invested boots of all.

“Imagine if we could reach out to a customer and just ask them: Is this really what you want to do? That's the magic. Nobody knows whether a transaction is real as well as the customer does. This intelligent friction is something to be welcomed. It’s all about finding the balance, you don’t want to bother the customer too much, but customers want to be in control, even when it comes to paying their existing beneficiaries. Authenticating the transaction instills confidence, and deputising the customer by giving them control builds trust,” he says.

According to Nolte, different types of fraud raises its head in different parts of the world depending on local conditions and standards embraced in that location.

“You see fraud move around the world. As it's solved in one place, it moves on to another market. Choosing the best standards is what keeps customers safe - and they needn’t even know it’s happening in the background. Sometimes you experience a kick back from your user base if their experience changes and so updating in the background is sometimes best,” Nolte advises.

Changing roles of financial institutions

Looking to the future, Nolte says that banks could leverage their position of trust as well as their unique access to user data to become the custodians of our consumers’ digital identities.

“Banks play a significant role in consumers’ lives. The trusted relationship between consumers and their financial institution means that banks are exceptionally well positioned to play a much larger role going forward. Instead of using my Google and Facebook to log in somewhere in the future, perhaps I can use my bank account, because that's where the anchor of my identity is,” he suggests.

Nolte, like many in his industry, believe there is room for industry standards when it comes to fraud detection and prevention. There is no reason why the best authentication should be a competitive advantage when it could be an industry standard. However, he says while this becomes a reality, organisations should waste no time in taking action.

“The tools are there, there is no reason to wait for the industry to define what should be done. You can’t be paralysed by worrying about how your customers will perceive the changes. Ultimately, if they are part of the solution and they know that they will be safer, they will be on board. The winning formula is to find someone to partner with who has done it before and done it at scale. Someone who knows the tech and knows what to expect. And even though fraudsters are constantly evolving and refining their techniques, we know that we can still make a massive dent in the damage they are doing. It’s all about having the right partner,” Nolte concludes.

About Entersekt

Entersekt is a leading provider of strong device identity and customer authentication software. Financial institutions and other large enterprises in countries across the globe rely on its multi-patented technology to communicate with their clients securely, protect them from fraud and serve them convenient new experiences irrespective of the channel or device in use. They have repeatedly credited the Entersekt Secure Platform with helping to drive adoption, deepen engagement and open opportunities for growth, all while meeting their compliance obligations with confidence.