

Companies win when the best security also means the best CX

Issued by [Entersekt](#)

12 Jul 2021

For many organisations, reaching customers through various channels has been a key focus over the last few years - especially as consumers started embracing more and more digital channels. But in order to truly optimise a customer's user journey, businesses should ensure a consistent experience across all channels. Consistency breeds familiarity, the saying goes, and it is especially important when it comes to the latest security measures that companies use to help protect their customers against fraud.

“Until now, omnichannel has simply meant offering multiple channels to the customer as a means to engage with a brand. However, this is no longer a competitive advantage in itself,” explains Pieter de Swardt, country manager for South Africa at Entersekt. “It’s about a well-crafted, seamless and consistent interaction between a brand and its customers, across all available channels. Not only can such an approach help lower chances of fraud across channels, but it will also result in increased customer trust,” he says.

Lack of consistency leads to confusion and frustration

According to De Swardt, before customer experience became the buzzword it is today, marketing professionals knew that consistency plays a key role in customer experience.

“Whether it is consistency in the brand message, or in how customers access services, we know that consistency builds loyalty and that loyalty generates revenue. With the rapid addition of digital channels over the past year - often out of necessity due to lockdown restrictions - many companies have neglected to ensure consistency, leading to confusion, frustration and even customer attrition,” De Swardt explains. “When we look at how customers are protected when they engage with these digital channels, the situation is even worse.”

According to De Swardt, a frequent stumbling block in the rush for digital transformation and a cross-channel service offering has been the disconnect between the different authentication methods used across different channels – even within one organisation. Not only do these inconsistencies detract from a customer’s overall experience, but he warns they can also create confusion about the security of each channel.

“Think of typical banking interactions, for example. When I log into online banking, I’m asked for a username and password. When I shop online using my bank’s credit card, I have to input details and then confirm with an SMS OTP. When I log into my banking app on my phone, I have to scan my fingerprint. And when I call my bank’s call centre, I’m asked a series of security questions - multiple times on some occasions. There has to be a more efficient and consistent way of doing this that wouldn’t leave the customer frustrated or worried about potential security weaknesses or fraud attempts,” says De Swardt.

The key is your customers’ hands

According to De Swardt, an omnichannel authentication solution can address this challenge and ensure a consistent experience across channels.

An organisation with an app, for example, can bind the identity of a customer to the app on their mobile device, enabling two-way communication through a mutually validated, end-to-end encrypted channel. The process transforms the mobile device into a one-touch, step-up authentication tool. “By making use of digital certificate technology within the organisation’s app, the customer’s mobile device itself becomes the key to unlock encrypted communications between the

customer's device and the organisation's servers. This means that an organisation would be able to send an authentication request to the device from their call centre, or from the browser for online banking logins, or from a merchant site for e-commerce transactions. No matter what action a customer takes they will always receive a message in their banking app asking them to confirm that it's them, or that they are approving a specific transaction. No variation. Absolute consistency. No matter the channel," De Swardt explains.

For companies that want to accommodate customers without smartphones, app-free authentication methods offering an equally high level of security and the same level of consistency are also available.

Specifically in the financial services industry, the move towards seamless, channel-agnostic experiences has caught on internationally, especially in the wake of the requirement for strong customer authentication under Europe's revised payment services directive (PSD2). De Swardt explains that banks have embraced solutions that can offer consistency, with Hanseatic Bank in Germany being the latest to [unify its authentication](#) processes through Entersekt and partner Netcetera's technology.

"The importance of consistency is not new. Ask any sports coach about the power of player consistency and you can expect a very long conversation. What many companies are discovering, however, is that customers want that same level of consistency when it comes to their digital security, too. In a world of uncertainty, consistency – especially in security – means more completed transactions. And that's money in the bank," De Swardt sums up.

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.

For more, visit: <https://www.bizcommunity.com>