Encap

Money 20/20 is about the ongoing changes in financial services, what was significant for your company in attending Money 20/20?

Money20/20 is an important event for Encap Security. It's one of the few 'fintech' events that gathers customers, prospects, partners and influencers from all over the world in one place. It is also a chance to check the pulse of the industry and see what is driving change, especially among major financial institutions.

This year security was hot again with 'risk, security and fraud' and 'biometrics' two of the official themes. While it's great that security is getting so much focus what I thought was significant was the lack of discussion around security as an enabler rather than a barrier or protector.

To explain - when it comes to security, the panel debates and conversations in hallways and at stands tended to focus on how to protect consumers and businesses from increasingly sophisticated hackers and fraudsters. This is of paramount concern but is still a narrow lens with which to view what new security technology can achieve.

Banks are trying to create a digital-first, omni-channel experience for customers. Challenger banks and fintechs are launching mobile/online-focused services designed to win the trust of business and consumers. With both groups investing heavily in new services, adoption is the measure of success. Banks need to meet the demands of a new generation of mobile-centric, loyalty-averse consumers and cut costs by shifting them to self-service channels. Fintechs need to acquire users and generate revenues in order to grow.

When consumers think of bank security they think of passwords and tokens, which by and large they hate. For organisations looking to drive customer adoption and use, security must enhance the user experience and help them engage with customers. It needs to transform from an inhibitor to an enabler of service innovation.

The discussion on this subject was significant by its absence.

What are the issues and challenges you are finding in the industry and how are you providing solutions?

One of the main issues is the red herring around standards. In my view standards are holding back banking security.

At Money20/20 it was clear that a standards-based approaches are in vogue with organisations such as FIDO Alliance and the GSMA with Mobile Connect pushing standards designed to reduce the reliance on passwords. With limited live-commercial implementations despite years of development, I question whether standardised approaches are right for banks, fintechs and consumers in the long run. After all, HSBC's voice recognition authentication for 15million consumers isn't standardised.

Encap Security's Smarter Authentication platform is proprietary and deployed by banks and fintechs such as Santander and mydesq across the world. What they value is a platform approach which allows them use a range of authentication methods native to the smart device in combination – biometrics, behaviour, location, etc - to create a solution that is best suited to the context: the individual, the device and the transaction. Banks can employ an array of current methods, add future methods as they become available and even put customers in control of their authentication preferences.

Suddenly security becomes a point of differentiation in an increasingly crowded market. With a lack of market traction and question marks around differentiation, it could be argued that standards-based approaches are more of a hindrance than a help to banking security.

Going forward what are the trends and advancements that we should expect to see in financial services?

Recognition that security can be innovative and 'cool' rather than a necessary evil is growing.

To date security has always been a trade-off between convenience and security. Make it easy (e.g. user name and passwords) and you increase the security risk. Make it secure (e.g. fobs and SMSs with one time codes) and you frustrate users. The banking sector has always erred on the side of caution, ensuring security was as tight as possible. Unfortunately today's digital natives (not to mind the rest of us) won't accept having to copy and paste codes or carry around extra hardware.

Banks investing heavily in digital self-service channels need to ensure that access is simple and convenient without also opening the door to hackers and fraudsters. Otherwise that investment is wasted and customers are pushed towards the challengers and fintechs deploying the latest authentication technology unburdened by legacy infrastructure.

Now the native capabilities of smart devices can be used to offer superior authentication methods delivered at internet scale. Voice, face and fingerprint biometrics, device location data and behavioural analytics - and ideas not even imagined yet - can improve customer experience without compromising security. Customers and banks are no longer tied to specialist hardware or need to ask their customers to use complex passwords.

All of a sudden security becomes near-invisible and no longer a point of friction in service use. Some forward-looking banks have realised this, and I expect the rest catch on quickly.