

Neobanks and AI for fraud mitigation start to take center stage to support digital in GCC



Fadi Yazbeck is the product manager for Temenos IslamicSuite. He can be contacted at fyazbeck@temenos.com.



We now live in a digital world. According to a report by emarketer, smartphone penetration is 83% and 73% of the UAE and Saudi populations respectively. Digital means instant, transparent and seamless and increasingly, Islamic banking customers expect their bank experience to also offer this approach. Banking should be no different to interacting with those services that support our digital lives such as Amazon, UAE ride-sharing service Careem, and Google, etc. Fail to offer an intuitive, similar banking experience and you fail to meet the expectations of the new tech savvy Generation Z audience that are soon to be your dominant target customers. Digital Islamic banking isn't the future, it's the now, but there are risks.

Cybercriminals love digital, in fact, smartphone platforms are the second most targeted platform by hackers after Windows. The GCC in particular is being hit hard. PwC's 2018 survey Pulling fraud out of the shadows: A spotlight on the Middle East, highlights that fraud and economic crime has increased 12% in just two years. And digital banking is taking a major hit; according to 2017's Norton Cyber Security Insights Report, 29% of UAE respondents had payment information stolen from their phones last year.

These are frightening stats for the region but it is not taking this issue lightly. At the very end of October, Saudi Arabia's King Salman issued a decree to set up the National Cyber Security Authority focused on enhancing the kingdom's existing cybersecurity efforts and protecting its "vital interest, national security and sensitive infrastructure". The following month Jeddah-headquartered OIC launched its own cybersecurity center. These are just a few examples of how the end of 2017 saw a major focus in fighting cybercrime within the region, but has this focus continued into 2018 and what does the future hold?

Review of 2018

The end of 2017 saw the emergence of some GCC banks make a confident move into the digital space by delivering separate neobanks such as Mashreq Neo and Liv bank. Neobanks sit on a 100% digital and mobile platform with no reliance on branches. To target this growing Generation Z market, they aim to offer an intuitive user experience platform (UXP) that feels familiar with other digital lifestyle interactions. Their systems are 100% new too, and so the cumbersome legacy of limited, inflexible back-end core systems is avoided. And when teamed with a real-time fraud solution that connects seamlessly to the core banking platform, this ongoing threat of fraud related cybercrime can be easily mitigated. However, this benefit isn't unique to these streamlined neobanks as all can benefit particularly when using advanced technology such as machine learning to detect fraud at initiation or during processing of a transaction.

Despite all the previous years' hype surrounding artificial intelligence (AI), 2018 became the year that the benefits of AI are finally starting to be realized in combatting cybercrime, and particularly fraud. At Temenos for example, 2018 has seen the launch a new real-time fraud solution which uses AI to profile individual behaviours and detect this common type of cybercrime. Developed to combat this growing risk that the new digital environment offers, banks need self-learning capabilities, beyond rules-based engines, to

profile customer behaviour, using vast amounts of customer data and transactions to flag activities outside behavioral patterns that could be a potential fraud. We are also working toward using cloud computing to deliver new algorithms that help solve the real-time fraud detection challenge.

Unfortunately, the stats for 2018 within the UAE in terms of cybercrime indicate that few are currently managing to combat fraud despite recent advances in technology. In early October, the former head of the one-day court in Dubai, Judge Ayman Abdul Hakam, highlighted that cases of electronic fraud are on the rise across the UAE.

Preview of 2019

2019 will see the software to combat cybercrime in general using elements of AI to address increasingly complex fraud threats and a greater push toward digital including neobanks becoming mainstream. McKinsey's Digital banking in the Gulf research on urban consumers in the UAE and Saudi Arabia showed that digital banking is unsurprisingly set to be popular in the region, with at least 80% of consumers now preferring to do a portion of their banking on computers, smartphones, and tablets.

Bahrain-based Bank ABC plans to launch a neobank early 2019 and many of our clients in the region, such as Al Salam, are able to offer the same benefits of a neobank having undergone a full digital transformation. Mohammed AlShehabi, the head of innovation from Al Salam Bank, said: "We recognize the need to offer a truly digital service to our clients, one that will evolve with their changing needs at an individual level. Offering value added to our customers is a must today, but trust and security ensure and form the indispensable base."

Conclusion

Cybersecurity is vital to the business world, ranking as the top priority for more than 36% of CEOs worldwide in their digital transformation, according to IDG's State of the CIO 2018 report, and yet it continues to increase within the GCC and beyond. The impact of this increase to Islamic banks is colossal; falling share prices, fines, reputational and client/partner relationship damage etc. It also means more pressure on systems and processes to accurately identify these. This means increased operational costs and more time spent on identifying fraud. In this developing digital environment, where we live in a real-time world, fighting sophisticated cybercrime schemes can be a struggle but it doesn't have to be. Real-time fraud solutions that utilize AI along with Shariah compliant core banking, are available regardless of a banks implementation strategy and Islamic banks can win this fight, but only if they are prepared. 📌