Fraud management in Africa's mobile market

By Gareth Whitaker

18 May 2016

With mobile ownership in South Africa and Nigeria now as common as it is in the United States, the continent is rapidly gaining ground as the new frontier for mobile. Its young population, ready to embrace the new mobile innovations and technologies, has attracted the attention of investors and innovators - as well as cyber criminals.

©prykhodov via 123RF

Global attitudes and trends company, Pew Research Centre, notes in its 2015 report that mobile phone networks have transformed communications in sub-Saharan Africa (SSA) to the extent that many on the continent have managed to leapfrog the landline stage of development right into the digital age. As such, Africa is ripe for digital opportunities.

Its youth population – predicted to increase by 42% in 2030 according to the United Nations – is believed to be a catalyst for economic growth, opening new markets on the continent with the information and communications technology sector at the forefront. According to April's 'Mobile Report for 2016' by the Mobile Marketing Association for South Africa (MMASA), 96% of the South African population are cellphone users.

In other sub-Saharan Africa countries such as Nigeria, Senegal, Kenya and Ghana, cellphone usage is also high where text messages, videos and photographs feature prominently. For those that are smartphone users, mobile money transfers are common in countries such as Kenya while social media access or access to news and information are more popular.

Capitalising on cellphone risks

However, like any other technology involving the transmission of personal information or transaction of any sort, comes challenges such as fraud prevention. While the MMASA reports that there are 4 million smartphones used for banking, the Ombudsman for Banking Services notes that in 2013, the number of cellphone phishing cases rose by 27% during 2013.

Other forms of fraudulent activities have occurred through SIM swapping, smartphone malware, network porting and spoofing. These call for mobile banking software security where the onus is now on financial institutions and wireless service providers to address risks and threats to electronic financial transactions and the transmission of financial information.

The age of data and software protection

With fraud detection software, many are able to detect and track unusual banking patterns and, with that, sound the alarm for any fraudulent activity. This is achieved through analysing real-time data so as to understand customer behaviour and to easily identify activities that are not their usual. Some intelligence tools are able to tell what happened, what is happening at present and what is about to happen, helping financial institutions to instantly react and follow up on unusual activity.

As mobile technology is driving fraudulent transactions, financial institutions are faced with the massive task of flagging potential fraud within the millions of transactions which take place daily and stopping the fraud within less than one second. When only 0.3% of those less than one-second windows are missed, research has indicated that one of the top-four, multinational credit companies could suffer losses of more than $10 million yearly (+- R150m). With losses like that, meeting 99.7% of Service Level Agreements (SLAs) is just not good enough.

Metrics-based solutions

Reducing the percentage of missed windows from 0.3% to 0.005% has the potential to reduce losses from more than $10m to under $200,000 (+- R3m). Therefore, financial institutions need solutions that can identify suspicious behaviour based on metrics such as location, transaction size and transaction frequency in real-time. Most importantly, these solutions need to stop the transaction before the 'customer' has left the store with the merchandise.

To achieve this, such solutions must be able to combine current, real-time metrics from big data sources with historical data to identify fraud patterns quickly, yet effectively. The key to combatting fraud lies in being able to have a holistic view of the transaction – typical behaviours, the black list of bad credit card numbers and real-time analytics that reveal new fraud patterns - within milliseconds. Without the ability to reduce online fraud, a financial institution’s assets, reputation, compliance and profitability are all on the line.

This highlights the crucial need for fraud management solutions, as companies are able to control their costs and prevent revenue loss while simultaneously increasing consumer confidence.

ABOUT THE AUTHOR

Gareth Whitaker, Presales Director at Software AG South Africa