Where Finance Meets finews.asia

Banks Need Hi-Tech Software to Mitigate Explosion in Fraud

Monday, 19 November 2018 05:42

Banks in the region facing escalating fraud need software with machine learning and advanced data analytics capable of spotting wrongdoing in real time, Raffael Maio of NetGuardians writes.

Raffael Maio is the Chief Operating Officer at NetGuardians

Financial institutions across Asia Pacific face a rising tide of fraud. According to EY, the variety and sophistication of cyber-attacks have all increased exponentially over the past two years in the region.

In real terms, this translates to hundreds of millions of dollars being stolen. This summer, for example, the UN estimated that cyber-crime was costing the ten countries in the Association of Southeast Asian Nations (ASEAN) alone between $120 million and $200 million a year – a sum that is taking its toll not just on the bottom line but also on reputation and trust.

Fraud Erodes Trust

One of the main tasks of a bank is to protect customers' money. When it fails to do so customers look elsewhere – at best curbing its ability to grow; at worst causing it to fail.

According to the 2017 ‹Fraud Management Insights Report›, banks in Vietnam, China, Hong Kong, Thailand, Singapore and Indonesia have some of the lowest trust scores anywhere in the world. Indonesia had the lowest score at 2.9 out of 10, China and Hong Kong scored 3.87 and 3.8 respectively, while the global average was 4.95.

A Worldwide Problem

Fraud is undoubtedly a worldwide problem, but as our recent white paper ‹Combating Financial Crime in Asia› points out, Asia Pacific faces its own challenges stemming not least from the recent rapid take-up of banking services and the widespread adoption of e-banking and mobile banking in particular.

NetGuardians
Combating Financial Crime in Asia
The Case for Advanced Data Analytics
Download white paper

Challenges of Mobile Banking

The lack of cyber-security investment, skills shortages, and also the pressure to bring new services to market fast have left banks across the region particularly vulnerable. Furthermore, bribery is still seen as a normal part of everyday business, inhibiting the development of anti-corruption corporate cultures.

Meanwhile, many regional regulators – a major driving force elsewhere in cyber-protection – have provided only limited guidance on managing operational risk.

The result is that few institutions use automated anti-fraud systems, with the vast majority relying on manual, Excel and paper-based approaches that are slow, expensive and proving incapable of preventing the explosion of fraud in the face of mounting transaction volumes.

Vulnerable Population

The challenge is exacerbated by the fact that the much of the region's population is unschooled in the scams of the fraudsters, leaving them highly vulnerable to phishing exercises and viruses, both commonly used to gain access to people's bank accounts. The authorities in Vietnam, for example, estimate that 72 percent of the country's smartphones are infected with a virus.

Scams are perpetrated through bogus apps that offer coupons for free meals, discounts and free games. Once smartphones are infected, the viruses enable the criminals to get to work, with the frauds often remaining undetected for months and even years, hidden behind the huge volume of genuine transactions.

Hidden in Plain Sight

A typical customer makes hundreds of mobile payments each month – many of very small value. The sheer volume makes it difficult to spot suspicious activity manually particularly as merchant names are not always easily relatable to a transaction. This complexity and volume is a godsend to fraudsters. By taking a little regularly from many people, they can net huge sums and remain under the radar. Things are starting to change.

Where not so long ago the level of fraud was seen as a manageable cost of business, today it is not. Some authorities have developed campaigns to help educate the population about phishing, but education on its own will not be enough.

Real-Time Prevention

Banks need anti-fraud software with machine learning and advanced data analytics such as NetGuardians' NG|Screener. By analyzing data for every transaction – such as screen resolution, location, payment destination, timing, amount and more – NG|Screener builds 360-degree customer and employee profiles, spotting and stopping irregular activity in real time, before the cash has left the account.

But that's not all. It throws up 83 percent fewer false alerts, cutting fraud investigation time by 93 percent. And in trials on historic data it found 18 percent more fraud that had previously gone unidentified. The result is that fewer transactions are blocked, an improved customer experience and an enhanced level of protection.

Banks Are Starting to Take Note

In Singapore, for example, they are moving from seeing fraud-mitigation software as a «nice to have» to a «must have». But localized implementation is not enough to rebuild and retain customer trust.

It must be implemented widely and systematically across the region hand-in-hand with a cultural shift towards zero fraud tolerance. Only then will we see fraud rates decrease as banks offer customers the kind of protection they deserve.

- *If you would like to learn more on this topic, download the white paper ‹Combating Financial Crime in Asia›.*