FOUR QUESTIONS TO DETERMINE IF YOUR FRAUD APPROACH FITS MODERN BANKING DEMANDS

Modern banking has evolved into an always-on, omnichannel operation. From opening an account, to checking an account balance, to making a purchase with a mobile device, customers expect a frictionless, secure interaction. But now that 70 percent of banking interactions are digital and newer innovations like real-time transactions and open banking are gaining popularity, fraud potential has increased and the time to evaluate risk has greatly diminished.

When banks fail to predict and prevent fraud, customers know. One in three respondents to FIS' 2019 Performance Against Customer Expectations (PACE) survey said they've been a victim of financial fraud. Further, 72 percent who had experienced fraud in the last year switched from using cash and cards for payments to using a mobile app.

In addition to customer transaction security, banks must predict, prevent and immediately respond to the sophisticated financial crimes like money laundering, internal theft and cybersecurity breaches, across the entire enterprise. Over the last decade, financial institutions have been fined nearly $20 billion in anti-money laundering (AML)-related penalties. Fraud-based crime has cost banks as much as $183 billion, and cybercrime an astounding $3 trillion.

As importantly, banks that fall victim to financial crimes face potentially irreversible reputational destruction. For many, this can become an impossible image to reverse.

With fraudsters coming at today's bank from every direction, advanced financial crime management technologies must protect all channels, and deliver the intelligence to predict fraud attempts before they happen.

Consider these four questions to ensure your financial crime management strategy is still a fit given the demands of modern banking:

1. **Can you respond urgently, enterprise-wide?**
   Banks must know about threats when they arise and have the power to take immediate action across the entire enterprise. You don't have the luxury of stopping operations when fraud or the threat of it is detected. An avalanche of transactions continue – from branches and call centers, ATMs, at the point of sale, and over the internet and mobile devices. This demands an enterprise-wide fraud management solution that concurrently analyzes millions – or even hundreds of millions – of records across every channel. To be effective, this analysis must occur in real time and instantly return suspicious results.

2. **Can you address different types of fraud by channel?**
   Fraud works differently based on the channel; criminals target internet and mobile transactions with different tactics. "Different channels and modes of fraud perpetration require analytical models tailored to each," explains Jwahar Bammi, principal solution architect, FIS. "If the solution you choose doesn't have all-encompassing, channel-specific analytical models built in, you are just as vulnerable to financial crime as you ever were." Cross-channel fraud is emerging as an advanced form of attack where a stolen identity is harvested to commit fraud across multiple channels. Fraudsters will look for the weakest link in the security chain to gain entry then commit frauds on multiple channels.

3. **Are your data analytics meaningful and usable?**
   Banks handle massive amounts of data that can be mobilized to thwart financial crimes – but to be effective, the information must be in usable and actionable format. The enterprise financial crime management solution you choose should be data scheme-agnostic, not reliant on storage databases (which can become expensive and unwieldy), and able to easily integrate disparate information sources. It should also have the ability to analyze data links and visually present the information in a manner that's easily interpreted.

4. **Are you using artificial intelligence and machine learning?**
   Artificial intelligence (AI) and machine learning (ML) are highly powerful tools in predicting and identifying financial crimes. Though often used interchangeably, they're not one and the same. AI refers to machines carrying out tasks in a "smart" manner; ML is a subset of AI that gives machines access to data and lets them learn for themselves. Yet, many enterprise financial crime management solutions cannot distinguish between AI and ML. This limits their capacity to combine different techniques – which is necessary to effectively prevent, predict and identify financial crime.

Don't react. Outsmart.

When you can predict financial crimes in every channel, you regain power over fraudsters. With highly scalable machine learning and AI capabilities, FIS Memento spots fraudulent transactions across your entire firm in real time and predicts new threats. Plus, you gain all the cross-channel tools your staff needs to efficiently and holistically manage any threat. It's just one of the reasons FIS has ranked No. 1 on the RiskTech100 list four years running.

TO LEARN MORE ABOUT FIS' INNOVATIVE FINANCIAL CRIME MANAGEMENT SOLUTIONS, click here OR CONTACT getinfo@fisglobal.com.