NICE Actimize

Protecting Banks against Fraud and Cybercrime with Analytics

Financial institutions' IT departments have virtually transformed many banking processes, turning to sophisticated data and analytics methodologies to gain an edge against their competitors while safeguarding their customers against financial crime. With the rise of online and mobile banking fraud and cyber-attacks, banks are concerned about fraudsters who exploit vulnerabilities created within the evolving digital environment.

Known for its enterprise fraud and cybercrime prevention solutions that fight against these challenges, NICE Actimize was started more than 15 years ago with a great analytics engine and best-in-class trading surveillance and case management solutions for investigations. Today, NICE Actimize is an enterprise fraud market leader in terms of the number of digital banking customers and transactions it guards within the United States, protecting more than 150 Mn U.S. digital banking customers across the top five U.S. banks.

"We are proud of our industry-leading enterprise fraud solutions that work hard to stop cyber-criminals before they gain access to bank accounts," said Mary Ann Miller, Senior Director and Fraud Executive Advisor for NICE Actimize. "We help financial institutions protect their customers by connecting the dots between fraud and cybercrime data for a holistic view of threats."

A core objective of any analytics solution is to deliver sustainable business performance and insights into markets, customers and in-house internal processes. NICE Actimize provides decisions and scores that can be acted on, with data and those outcomes rich in information that can be used to uncover fraud as it is happening in real time. The fraud solutions provider also uses rich analytics models to enhance customer experience by avoiding unnecessarily blocking users from legitimate transactions.

> " NICE Actimize's open analytics technology allows financial institutions to easily design their own fraud detection or risk models and stay ahead of emerging fraud threats "

In light of the recent data breaches, fraudsters have shown that they have no problem gathering reams of personal data which they use to pass authentication hurdles by changing passwords and other account information to takeover and access funds. Miller cites, "The good news is that our fraud solutions employ behavior analytics and very quickly spot unusual patterns that indicate account manipulation and takeover. This is our sweet spot. NICE Actimize's open analytics technology allows financial institutions to easily design their own fraud detection or risk models and stay ahead of emerging fraud threats."

Another perfect example of the need for open analytics was the release of Apple Pay. "When the wallet first went live, fraud became rampant within a

Mary Ann Miller

matter of days," explains Miller. "That fraud was linked to the provisioning of cards onto the mobile wallet – something that wasn't foreseen. We had our customers put our open analytics approach to work, building fraud detection models that specifically sought out unusual behavior linked to the provisioning of cards onto Apple Pay. These users experienced no fraud losses while many in the industry were bleeding."

What is in NICE Actimize's future? The company is laser-focused on providing further innovation in authentication management, using advanced analytics to make real-time, risk-based decisions that enable legitimate customers to transact easily, while keeping the fraudsters out.

Miller concludes, "Our recent Customer Satisfaction surveys displayed a high level of confidence in our fraud solutions, and we feel that our precision analytics, in addition to our support services, is a contributing factor to this result." **BC**