www.financialit.net • March Issue 2016

Financial IT

Innovations in Technology

Mary Ann Miller
Senior Director, Fraud Executive Advisor and Industry Relations, Nice Actimize

FACING DOWN PAYMENTS FRAUD

Connecting the Dots: the digital transformation of risk analytics and decision-making

Paul Thomas,
Managing Director
of Provenir

The IT impact on the evolving financial trading landscape

Darren Watkins,
Managing Director
of VIRTUS Data Centres

The easing of sanctions against Iran

Farhad Alavi,
Managing Partner
of Akrivis Law Group, PLLC

Financial IT

FACING DOWN PAYMENTS FRAUD

Data analytics play a key role

This year's payments and financial services industry events are facing down a range of critical protection issues emanating from new directives and transaction protection issues. With the rise of online and mobile banking fraud and cyber-attacks, banks more than ever are concerned about fraudsters who exploit vulnerabilities created within the evolving digital ecosystem.

First up for discussion is the recently updated Payments Services Directive (PSD2), adopted by the European Parliament last October, which requires traditional banks to open their doors to new technologies so that Third Party Payments (TPPs) providers can offer alternative financial services. With PSD2, regulators are enforcing innovation and competition in the payments world.

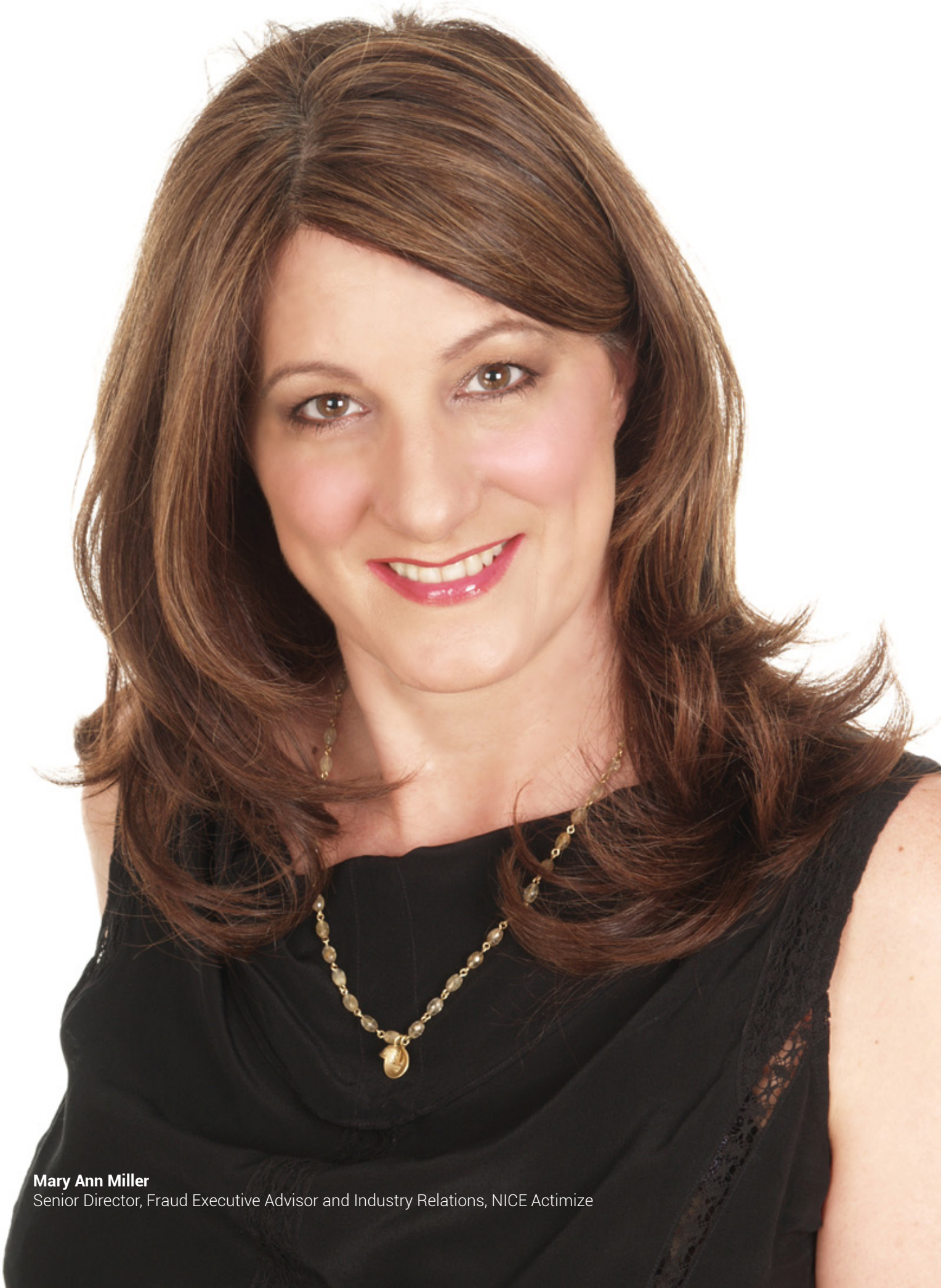
While financial institutions are certainly keeping an eye on the competitive landscape, for now they're possibly even more focused on the demanding details of the technical standards they will have to meet. PSD2 doesn't just enforce competition in payments: it demands safety in providing such innovative services. As such, the regulations require financial services providers and third-party providers alike to apply "strong customer authentication" using a two-factor strategy for every single digital transaction. That means financial insitutions must combine two methods of authentication, choosing from three different categories of tools that confirm, "something you know" (password), "something you have" (token), and "something you are" (biometrics).

Post Apple Pay Thinking

Aligned to this, is how financial institutions are applying the lessons learned from the launch of Apple Pay to other payment scenarios. Will PSD2 bring the same fraud disaster as Apple Pay provisioning? PSD2 requires banks to open an API to customer accounts and data and will result in scenarios similar to those that occurred when card-based mobile wallets launched globally. The launch of Apple Pay was a "pure delight" to fraudsters and the industry saw the highest basis points of fraud in many decades. We must remember that at the end of every fraud, is a consumer whose customer experience, along with the perceived safety of their money, impacts their overall satisfaction with their financial institution.

PSD2 tries to address fraud with strong authentication regulations that take a bit of a "silver bullet" approach to the subject of cyber-crime and fraud. So, with this well-documented fraud history in mind, do we work as a "safe payments" community to create an informed data exchange, solution analytics and multilayered approach to PSD2 that allows changes to the cyber-fraud threats to pivot with the changes in the environment? That does seem to be one solid approach to the problems faced.

The truth is that good cyber-fraud strategy is possible, but not as an afterthought or as a one-time effort. Strict regulation of strong authentication only sends the strategy down a" tail chasing" route and does not allow for new ways of protection and innovation on the cyber-fraud risk side of the house. Not only are we looking at events like money movement, enrollment, log-in and every kind of payment device you can imagine, but along with the ongoing evolution of the product, third-party providers should address their customer demands with strategies and solutions



Mary Ann Miller
Senior Director, Fraud Executive Advisor and Industry Relations, NICE Actimize

that include payment safety and security elements.

Data analytics – second nature to financial IT providers

Moving past regulation to the importance of data and analytics in a sound and balanced fraud strategy –recent discussions have centered on which approach really works best. Of course, these topics are certainly second nature to the financial IT community, but there are many varied points of view on how to implement them. Open channels of data exchange in a common context would be ideal to an informed analytics and scoring strategy for cyber-fraud risk with PSD2. Not only open channels and common context, but open platforms on both the bank and financial IT provider's side would permit the exploitation of the value of data to protect the end-to-end transaction.

The "open" ability to create models for specific attributes provides the capability for creative cyber-fraud analytics development that ultimately will support rapid product launches with a competitive advantage. This open analytics approach also can enable passive or managed authentication for PSD2, which can be cost effective and in the end would certainly get applauded by consumers.

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

These rich analytics are the key way to stop account takeover. Very often fraudsters may commit account takeover by changing a phone number through a call to the contact center. Then they may wait a few days before they initiate money movement. Our analytics aggregate scores which show when things have gotten truly serious enough to block.

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 take over and access funds. The good news is that today's fraud solutions employ behavior analytics that very quickly spot unusual patterns that indicate account manipulation and takeover. Additionally, open analytics technology can allow financial institutions to easily design their own fraud detection or risk models and stay ahead of emerging fraud threats.

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

These trends and discussions on fraud and payments bring us to a crossroads – as we demonstrated with the Apple Pay story, delivering a good customer experience is an important element to what we all consider success. The same kind of "creative juices" that are used for product innovation for financial IT payment solutions should also be brought to bear on the customer side of the equation. This is a weak solution that allows an open season for cyber-fraudsters is no good, but neither is a solution that presents security barriers for customers. We think there are ways to the desired results on both sides – cool tech can and must live with a great customer experience.

Finally, precision analytics work together with strong support services at both the financial institution and technology vendor side, as a contributing factor to a desired end result. At the end of the day, our objective is to protect customers by connecting the dots between fraud and cybercrime data for a holistic view of threats. We have a unique opportunity to get the right balance that provides a winning solution for both the financial institutions and the customers they serve.

Mary Ann Miller

Senior Director, Fraud Executive Advisor and Industry Relations, NICE Actimize

Mary Ann Miller, Senior Director, Fraud Executive Advisor and Industry Relations, NICE Actimize, is a global authority on enterprise fraud and risk management. Leveraging more than 20 years of experience and extensive knowledge in decision analytics, operational excellence, and customer centricity, Ms. Miller consults with financial institutions worldwide to establish business and technology strategies pertinent to the cultural climate and individualized business needs. In her previous directorships and executive roles in fraud strategy at USAA, eBay/PayPal, and Lloyds Banking Group, Ms. Miller provided a strategic business perspective on establishing financial crime analytics across the enterprise. She has also guided cross-functional teams in complex fraud implementations designed to minimize criminal activities.

Follow Ms. Miller at the NICE Actimize blog: http://www.niceactimize.com/author/Mary-Ann-Miller or on twitter at @CyberGalMAM.

NICE · ACTIMIZE

Market Leading Fraud Risk Detection & Prevention Technology

Contact Centre Fraud | Deposit Fraud | Real-Time Payments Fraud Detection for Retail, Commercial, and Private Banking | Card Fraud | Employee Fraud

Effective fraud risk management requires a real-time, customer-centric approach. NICE Actimize provides proven solutions, which reduce fraud losses, mitigate reputational damage, and increase operational effectiveness and efficiency.

Profiled Vendor
2015 CEB TowerGroup Enterprise Fraud Management Update

Category Leader
2014 Chartis RiskTech® Quadrants, Enterprise Fraud Technology Solutions

Recognized Provider
2014 Aite Enterprise Fraud Management Market Impact Report