NICE · ACTIMIZE

Steps to Prepare for Faster and Instant Payments

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

Steps to Prepare for Faster and Instant Payments

Key elements to supporting a faster payments environment

Nations the world over are moving to faster and instant payments. In some nations, FIs will usher in many kinds of instant and faster payments in both retail and commercial settings.

This shift will introduce a world of exciting new products and services in banking, but it will also pose new fraud and operational challenges.

FIs will need to focus on fraud strategies that provide rich analytics that enable detection for a range of payment types. Actimize suggests a multi-layered strategy, which includes dynamic and intelligent authentication management, rich and adaptive behavior analytics, and operational systems that are tailored to support and prioritize faster payments products and services.

Intelligent Authentication Management

Fraud prevention starts at the very point where consumers – and fraudsters – initiate transactions. As a result, it is important to implement risk-based authentication which enables real-time decisions and the ability to choose the right authentication method for instant payments.

Intelligent authentication management, including the following capabilities:

- Risk-based decisions at log-in and throughout a session for each interaction
- Management of many authentication methods across channels, making appropriate step-up decisions among these tools based upon risk, cost efficiency or customer preference
- Authentication strategy that is built specific to faster payments, with the ability to write rules to leverage more stringent authentication for high-amount, fast transactions, for example and agility in modifying rules.

Analytics and Fraud Risk Scoring

As FIs transition to faster payments, they'll need to rely on fraud detection tools that use behavior analytics to identify risk in real time.

These tools build customer-level profiles to establish a baseline of normal or typical behavior and then spot anomalies indicative of fraud. Anomalies might include a combination of new payees, in suspicious regions stemming from an unusual user device, for example.

The fraud detection tools also monitor channel data and have a deep understanding of monetary and non-monetary events – such as changes on the account servicing.

The desired output of these analytics is a fraud risk score that combines all the vectors of the customer activities relating the transaction, the event, the channel and device information, and behavioral history between the counterparties.

Fraud Strategy Rules for Faster Payments

Generating fraud risk scores is an important first step, but must be supported by strategy rules that are designed specifically for a faster payments environment.

Fraud strategists should be able to write simple business rules, so that payments and risky events can be automatically actioned in real time – such as delaying a payment, or introducing a step-up authentication, or referring the transaction to an analyst for manual review.

It's important for an organization to determine their risk appetite on faster payments weighing security and customer experience – and then write rules accordingly.

Operations and Case Management for Faster Payments

Lastly, a fraud management system needs to have a central alert and case management system which enables the prioritization of faster payments alerts. This gives FIs the ability to start investigations and create cases in a separate workflow – combining many related activities for investigation.

This approach should include dynamic reporting from investigations linked to appropriate customer outreach.
All-in-all, as payment methods speed-up, it is critical to streamline fraud management processes so that fraud risk analysis can happen immediately, and decisions can be automated, reserving the human-element for the most risky manual review of prioritized alerts in real-time.

Conclusion

Fraud concerns linked to faster payments are to be expected – but these changes are inevitable.

The best way to prepare for the potential uptick in fraud threats linked to faster payments is to have a strategy in place before you implement new services. It will be much simpler to tweak and alter fraud controls according to need than it will be to begin implementing systems after attacks are in full force.

This is the time to assess your current fraud controls and strategies, and then begin to build a plan.