White Paper

NICE ACTIMIZE

Secure & Compliant Real-time Payments

For Financial Institutions

NICE · ACTIMIZE

Contents

NICE · ACTIMIZE

INTRODUCTION

Real-time, digital payments have never been more pertinent for financial institutions. Even prior to the pandemic, megabanks offered their customers mobile banking and a variety of digital payment services, while financial institutions faced resource constraints that limited their digital offerings. Learn how to overcome these constraints and understand why now is the time to embrace digital banking and payments as a competitive differentiator.

This white paper:

- Explores the importance of real-time, digital payment services
- Explains the associated financial crime risks for various payment channels
- Defines tangible solutions in mitigating risks to safely serve customers and members

About Us

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.

NICE · ACTIMIZE

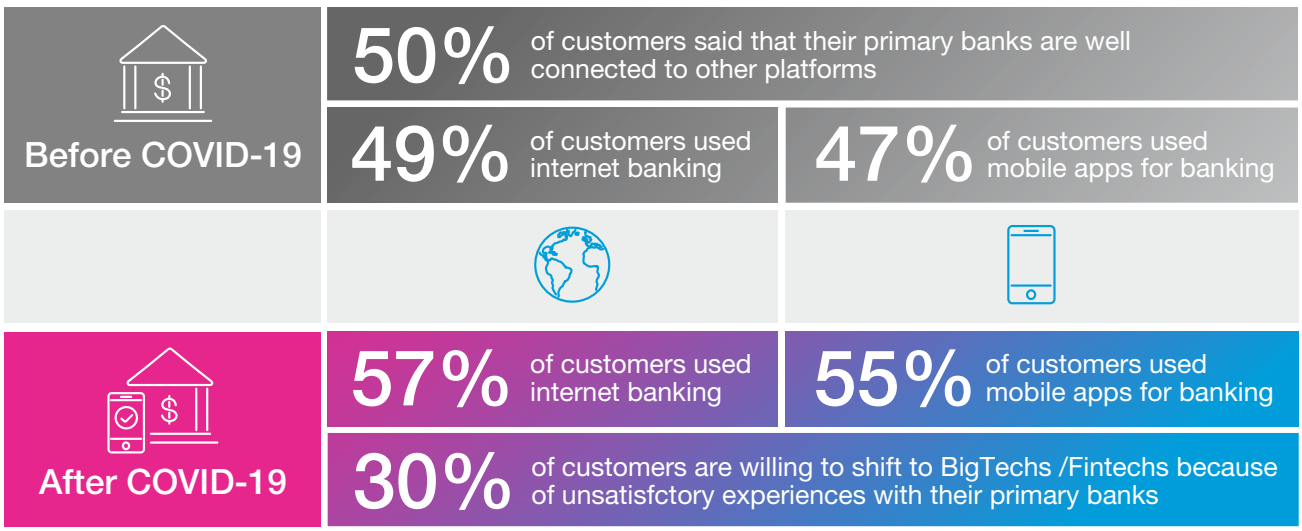
SECURE & COMPLIANT REAL-TIME PAYMENTS FOR FINANCIAL INSTITUTIONS

Why Real-time Payments are Becoming a Table Stake

COVID-19 is Accelerating Digital Transformation

COVD-19 has changed the way consumers approach banking and payments. While millennials – who will represent half of the U.S. population in 2021 – have already embraced digital banking and real-time payments, the other half will continue adopting these digital channels post-pandemic.

COVID-19 Driving Consumer Behavior Changes in Banking



Source: The Financial Brand, June 2020

According to the Financial Brand 2020 survey:

- 31 percent of respondents will use online or mobile banking more in the future
- 45 percent of consumers have used a mobile wallet payment platform in the past 30 days
- There will be a measurable shift away from cash and checks
- More than 45 percent of respondents say they have permanently changed how they interact with their bank since COVID-19
- 40 percent said they will shop online more in the future than in a store

NICE · ACTIMIZE

Real Time Payment Network At-a-Glance

- In November 2017, The Clearing House launched the Real Time Payment (RTP) network, which provides real-time payment and settlement service to banks.
- As of January 2020, 21 large banks are in the network (Murphy 2020).
- The Federal Reserve is also currently developing a similar service called FedNow, which is expected to be available in 2023 or 2024.
- The RTP network and FedNow are intended to connect more than 10,000 banks across the country.

At a time where consumer trust is fragile, financial institutions must reevaluate their digital banking strategy to ensure they're creating a secure and convenient environment.

Faster Payments or Real-time Payments?

The shift to digital banking is here to stay, long after the pandemic. Consumers will increasingly adopt online and mobile banking, as well as increase online payments. As financail institutions gear up to strengthen their digital banking offering, they need to understand the nuances between types of payments.

There is a fundamental difference between faster payments and real-time payments. "Faster payments" could be referred to as any type of payment that is faster than a previous payment. For example, same-day ACH and card-network programs (Visa Direct and Mastercard Money Send) that send credit transfers over the card networks have payments that typically arrive in 2 to 30 minutes. The implementation of faster payments is still at an early stage, which means that every financial institution still has a decent chance to compete in the digital era.

By contrast, real-time payments not only have to post (making funds immediately available) but also immediately settle as opposed to batches at regular intervals such as in the ACH system.

To stay competitive, FinTechs and BigTechs have introduced alternate instant payments solutions such as Venmo and Square Cash, as well as other digital wallets like Apple Pay contributing to the high-expectations of mobile users for instant payments or transfers.

Unfortunately, criminals have exploited the instant nature of real-time payments. In 2020, there are at least 54 active real-time payments schemes in operation around the world covering almost all business banking models – including Business-to-Consumer (B2C), Business-to-Business (B2B), Consumer-to-Business (C2B), Domestic Person-to-Person (P2P) and Cross-border P2P.

As of June 2020, at least 16 billion records, including credit card numbers, home addresses and other sensitive information, have been exposed through data breaches since 2019. Just the first three months of 2020 have been one of the worst in data breach history, with over eight billion records exposed. This combination of massive data breaches and rampant COVID-19-related fraud schemes have broken the digital banking trust among consumers.

NICE · ACTIMIZE

Solution: Stage 1

Break away from rule-based models to improve your response time to same-day ACH payments. Adopt unsupervised machine learning models to autonomously monitor all credit and debit transactions to detect high-risk anomalies. Unsupervised machine learning models empower you to expand your fraud detection beyond known fraud schemes — widening your view on risks, while strengthening your understanding of each customer's behavior.

Solution: Stage 2

Take a layered approach by analyzing device attributes, geolocation, and behavioral analytics. Device attributes, such as IP address and browser type, help you understand the typical mode of access for your true customers. Analyzing geolocation helps you understand the origin of activities such as login, deposits and payment. Lastly, behavioral analytics should be woven throughout your entire fraud strategy. By building a behavioral profile for each customer, you're able to get a granular understanding of how each customer transacts — ensuring that alerts are only generated for true, risky behavior for each account.

With new technology, comes new risk. Stay informed to stay ahead.

Path to Secure & Compliant Real-Time Payments

Stage 1: Secure Same-Day ACH Faster Payments

Same-Day ACH provides consumers, businesses, government entities and financial instructions the ability to move money between bank accounts quickly.

However, with same-day processing, FSOs will need to review thousands of additional transactions per day. Fraudsters exploit data breaches to steal account information, perform authorized party fraud on ACH and bust out quickly. Conventional ACH fraud detection solutions use rule-based models that were built around known ACH fraud schemes. But these have proven be inefficient and ineffective, as they can neither detect new, unknown ACH fraud schemes, nor provide real-time intervention in preventing fraud losses before authorization.

Stage 2: Safeguard Mobile RDC Banking

While physical check payments have declined, checks have not become irrelevant. Remote deposit capture (RDC) has become a common and important component of the digital banking experience in the U.S.

An analysis of the check decline is very telling about why check may still be around for years to come. In the past 20 years, direct deposit replaced paper checks by the billions. Inexpensive card terminals all but eliminated checks at the retail point of sale. Online bill pay did away with billions of consumer-to-business (C2B) check payments. Prepaid debit card replaced another huge chunk of B2C checks. Even the introduction of Apple Pay, EMV chip cards and mobile wallets have not eliminated checks as a payment method.

NICE · ACTIMIZE

Once the check has cleared, there are three ways the fraudster gets the money out:

- The fraudster uses online banking to initiate a wire to transfer funds into one of their existing accounts at another financial institution.
- The fraudster asks the victim to send the deposited money by cashing out and then using a third-part money transfer service.
- The fraudster asks the victim to send a debit card, allowing the scammer to cash out at an ATM.

Solution: Stage 3

Invest in solutions that monitor all account activity and sessions prior to the fraudulent event. Many financial institutions still detect fraud at the point of transaction — which means they are dedicating resources to loss recovery, rather than loss prevention. Speed and real-time interdiction are must-haves for P2P payments. AI analytics allow you to consistently monitor session activity and take action on high-risk behavior, before incurring any financial loss.

As a result, financial institutions introduced mobile RDC as an option for consumers. Mobile, remote RDC is a service that allows a user to scan checks and transmit scanned images and/or ACH-data to a bank for posting and clearing via a mobile phone. Its popularity has made it one of the main entry points into mobile banking.

Mobile banking fraud via RDC impacts financial institutions of all sizes, and losses are escalating quickly. Victims are romanced on online dating sites or social media networks and provide their account information to the scammer. The scammer then sets up mobile banking for the account, including the ability to use mobile RDC and then uses RDC to make deposits into the victim's account, often using stolen, counterfeit or cashier's checks.

Stage 3: Protect P2P Payments in Real-time

Mobile payments have been part of millennials' everyday life but with the pandemic, mobile payments are now part of everyone's everyday life. Person-to-person or peer-to-peer (P2P) payment services are becoming increasingly popular for payment types, such as rent or splitting bills with a roommate.

B2C real-time disbursements can aid cash flow for merchants and consumers as well as supports gig economy "payroll by the gig" vs. "paycheck to paycheck" payment cycles. B2B cash flow, forecasting and cash management needs are the primary drivers behind the adoption of real-time payments where buyers and suppliers benefit from enhanced data and speed.

Zelle has been a popular P2P payment service among megabanks and is increasingly adopted by financial institutions. Offering this service not only better serves your customers and members, but it also keeps you competitive among your peers. However, Zelle payments are true, real-time payments; once the transfer is sent, it's gone. Zelle's speed in transferring funds has made it a prime target for criminals. It's important to note that the risk is not exclusive to existing Zelle users. Criminals spoof phone numbers to pose as a bank and request the consumers to verify their identity — typically asking the consumer to read the one-time passcode to the criminal. The criminal then accesses the consumer's account, registers for Zelle, and sends funds to a third-party account. Depending on the bank's daily Zelle limit, criminals can move anyhwere from $1,000 to $5,000 per account, per day.

NICE · ACTIMIZE

Solution: Stage 4

Build a unique understanding and behavior profile for each individual account. Applying a set of rules to a segment of "similar" customers doesn't work; alerts will be generated for scenarios where the behavior doesn't fit into the mold of the expected behavior for that segment. The only way to ensure low false-positives and friction-right experiences is to analyze insights at the individual account level. AI is a powerful tool to scale this across all your customer accounts and ensure the highest level of security — without compromising the customer experience.

Solution: Stage 5

Start by connecting fraud and AML insights through a unified case management system. This is an easy way to increase collaboration between the teams and work from a single workflow. As an example, fraud analysts can send confirmed fraud cases to the AML team, complete with case details, transaction details, and investigator comments. The AML analyst can then complete the investigation details for regulatory filing, such as a Suspicious Activity Report (SAR). By leveraging a unified case management system, analysts are working from one single workflow, increasing efficiency, and creating the most complete view of financial crime risk.

Stage 4: Enable Friction-right, Real-time Payments

Consumers and financial institutions alike see immense value in real-time payments – when done right. Consumers expect to be recognized and re-recognized with each digital interaction without experiencing any unnecessary verification steps. Security and fraud prevention is equally important and consumers place the responsibility on the financial institution.

Financial institutions must strike the right balance between customer experience and de-risking payments.

A lot is on the line for financial institutions; the speed and irrevocability of real-time payment schemes creates a "digital cash" experience, where payments are irrevocable and final and are immediately debited and credited to the sender and receiver.

Stage 5: Connect Fraud & AML to Stay Compliant

The lines between fraud and AML are blurring and megabanks have adjusted their financial crime strategy for a continuous view of financial crime. Many financial institutions still have separate tools, processes, and investigation for their fraud and AML teams. However, this siloed approach has created operational inefficiencies and an incomplete analysis of risk.

Where there's fraud, there's often money laundering. Criminals use money mules to launder funds — which is often traced back to fraud schemes, such as account takeover, check fraud, and wire fraud. When fraud and AML teams work in silos, analysts end up duplicating work because they were unaware of the other team's efforts. In scenarios where both teams are collaborating on a case, they communicate via email or phone — slowing down the investigation process.

Connect Fraud and AML to provide a holistic view of risk. End to End Fraud prevention will begin risk mitigation at the point of application by detecting and preventing the use of fraudulent identities; often used for money muling. In addition, fraud data is real-time, and by having a holistic view of risk; fraud detection is data rich and in real-time. By using fraud detection data as part of your AML tool kit you can accelerate the speed of which suspicious activity is detected by AML transaction monitoring as well.

NICE · ACTIMIZE

Accelerate Digital Transformation

COVD-19 has changed the way consumers approach banking and payments. While millennials – who will represent half of the U.S. population in 2021 – have already embraced digital banking and real-time payments, the other half will continue adopting these digital channels post-pandemic.

Bringing It All Together

Use AI and machine learning technologies to build a unique understanding of each individual account and monitor its transactional patterns. With AI-enabled analytics, you can increase granularity and ensure alerts are only generated for true, risky behavior for each account.

Your financial crime prevention solution should enable you to perform real-time, consistent analytics on:

- Device attributes to identify unusual activity
- Geolocation of deposits and withdrawals
- Frequency, time of day, amounts or speed of transactions
- Omni-channel activity across logins, account changes and movement of fund

To stay ahead of financial crime, financial institutions must increase collaboration across their investigation teams.

By connecting fraud and AML insights, investigators are able to:

- Work more efficiently from a unified case management system
- Assess risk through a single pane of glass
- Perform more thorough investigations, without duplicating efforts

Leverage an all-in-one, cloud platform to increase your agility against new threats. Stacking point solution on point solution only solves a small piece of the puzzle. This traditional approach requires you to toggle between different tools for each channel and requires additional interpretation of multiple risk scores.

A cloud platform allows you to:

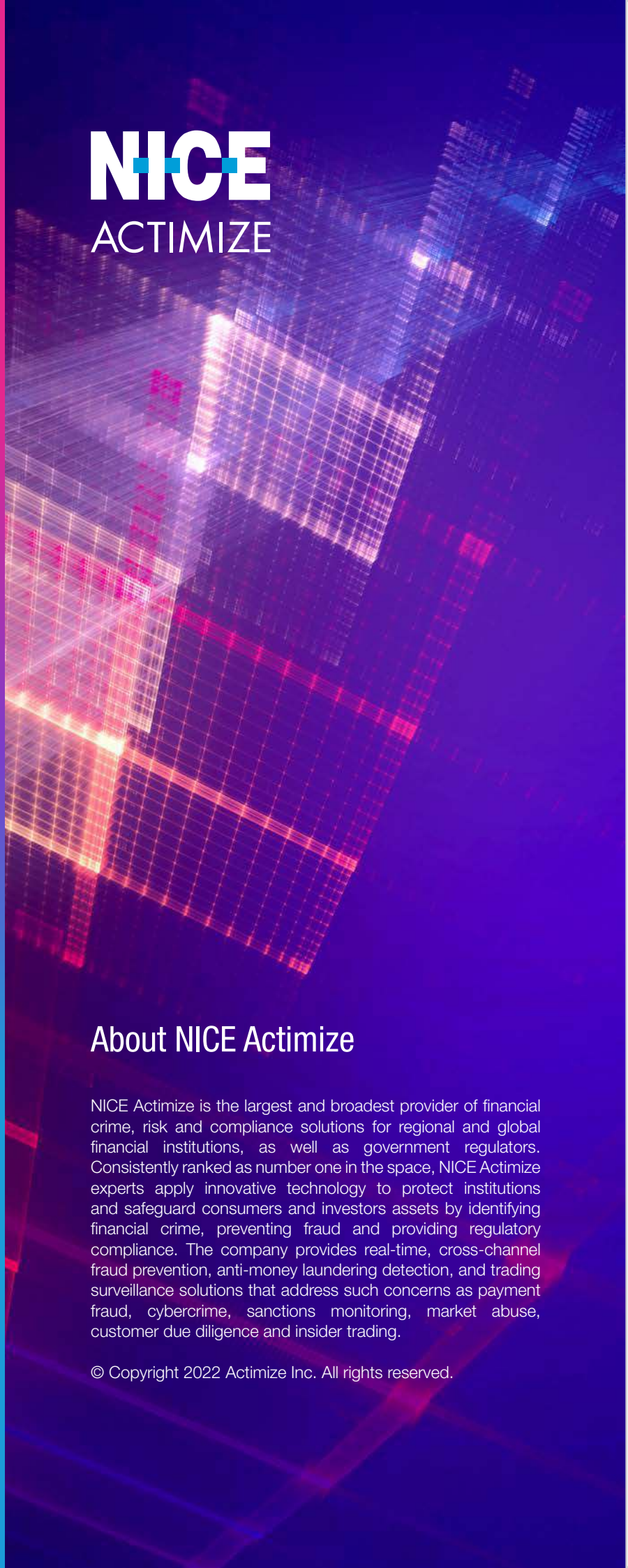
- Improve your speed-to-market
- Respond quickly against new attack vectors
- Centralize all tools, investigation and regulatory filing activities on one platform

Fast-Track Your Journey

Protecting real-time payments through artificial intelligence and machine learning technologies is easier than you think. IFM-X is the next generation enterprise fraud management platform that provides End to End Fraud Prevention that's powered by Always on AI to accurately detect and adapt to evolving threats. NICE Actimize was built with financial institutions in mind – empowering you to offer new digital payment services safely.

Get in touch to learn

how NICE Actimize can help fast-track your digital transformation journey



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.