



NICE Actimize 2026 Fraud Insights Report Identifies a Crucial Turning Point for Digital Fraud Detection

New research reveals fraud is hiding within trusted patterns as ACH fraud accelerates at nearly five times the payment growth rate

Hoboken, N.J., April 28, 2026 — NICE Actimize, a [NICE \(NASDAQ: NICE\)](#) business, has released the “2026 NICE Actimize Fraud Insights Report, U.S. Payment Fraud Edition,” spotlighting a pivotal shift in digital fraud: criminals are increasingly succeeding by blending into the very signals financial institutions have long trusted. Based on billions of transactions analyzed, the report shows why established detection strategies are reaching a turning point—and why financial institutions must rethink how they find and stop fraud before losses accelerate.

For years, digital fraud detection relied on two foundational signals: device risk and unfamiliar payees. Both are now eroding simultaneously. The primary driver is the rise of scam typologies that manipulate customers into authorizing payments themselves on their own devices, bypassing device-risk controls. Account takeover through session and credential compromise contributes further, particularly on web channels.

The report finds that detection strategies built on identifying new devices or newly introduced payees are losing predictive strength as a result. The report’s most urgent data point concerns ACH. Attempted ACH fraud value grew 52% in 2025 while total ACH payment value grew just 11%, a nearly 5-to-1 divergence. The average fraud attempt on the rail now exceeds the average payment value. Without targeted controls, the report warns that ACH could shift from secondary exposure to a primary risk vector.

“What makes the 2026 findings particularly significant is that fraud is not just growing. It is adapting specifically to defeat the controls financial institutions have invested in,” said **Craig Costigan, CEO, NICE Actimize**. “The institutions that will manage this environment successfully are those willing to challenge legacy assumptions, recalibrate their detection models and look beyond their own data.”

Additional findings within the report cover diverging fraud dynamics across domestic and international wires, P2P channels and check fraud. Domestic wire loss exposure is rising per transaction even as fraud rates hold steady. The report also finds that a single low-cost device model drove 3% of all mobile account takeover attempts. Finally, the report notes that web and mobile P2P fraud now require completely different detection strategies.

Addressing the challenges uncovered in the report, the [Actimize Insights Network](#) helps financial institutions address advanced digital fraud by providing the scale and precision needed to prevent losses before money moves, while supporting governance. Because criminals operate across institutions, financial institutions need intelligence beyond their own data. The Actimize Insights Network enables secure collaboration across institutions while maintaining the highest standards of data protection, privacy and regulatory compliance.

The full 2026 NICE Actimize Fraud Insights Report is available [here](#).

About NICE Actimize

As a global leader in artificial intelligence, platform services, and cloud solutions, NICE Actimize excels in preventing fraud, detecting financial crime, and supporting regulatory compliance. Over 1,000 organizations across more than 70 countries trust NICE Actimize to protect their institutions and safeguard assets

FOR IMMEDIATE RELEASE



throughout the entire customer lifecycle. With NICE Actimize, customers gain deeper insights and mitigate risks. Learn more at www.niceactimize.com.

About NiCE

NiCE (NASDAQ: NICE) is transforming the world with AI that puts people first. Our purpose-built AI-powered platforms automate engagements into proactive, safe, intelligent actions, empowering individuals and organizations to innovate and act, from interaction to resolution. Trusted by organizations throughout 150+ countries worldwide, NiCE's platforms are widely adopted across industries connecting people, systems, and workflows to work smarter at scale, elevating performance across the organization, delivering proven measurable outcomes.

Corporate Media Contact

Cindy Morgan-Olson, +1 646 408 5896, cindy.morgan-olson@niceactimize.com, ET

Investors

Ryan Gilligan, +1 551 417-2531, ir@nice.com, ET

Omri Arens, +972 3 763-0127, ir@nice.com, CET

Trademark Note: NiCE and the NiCE logo are trademarks of NICE Ltd. All other marks are trademarks of their respective owners. For a full list of NICE's marks, please see: www.nice.com/nice-trademarks.

Forward-Looking Statements

This press release contains forward-looking statements as that term is defined in the Private Securities Litigation Reform Act of 1995. Such forward-looking statements, including the statements by Mr. Costigan, are based on the current beliefs, expectations and assumptions of the management of NICE Ltd. (the "Company"). In some cases, such forward-looking statements can be identified by terms such as "believe," "expect," "seek," "may," "will," "intend," "should," "project," "anticipate," "plan," "estimate," or similar words. Forward-looking statements are subject to a number of risks and uncertainties that could cause the actual results or performance of the Company to differ materially from those described herein, including but not limited to the impact of changes in general economic and business conditions; competition; successful execution of the Company's growth strategy; success and growth of the Company's cloud Software-as-a-Service business; rapid changes in technology and market requirements; the implementation of AI capabilities in certain products and services, decline in demand for the Company's products; inability to timely develop and introduce new technologies, products and applications; difficulties in making additional acquisitions or difficulties or effectively integrating acquired operations; loss of market share; an inability to maintain certain marketing and distribution arrangements; the Company's dependency on third-party cloud computing platform providers, hosting facilities and service partners; cyber security attacks or other security incidents; privacy concerns; changes in currency exchange rates and interest rates, the effects of additional tax liabilities resulting from our global operations, the effect of unexpected events or geo-political conditions, including those arising from political instability or armed conflict that may disrupt our business and the global economy; our ability to recruit and retain qualified personnel; the effect of newly enacted or modified laws, regulation or standards on the Company and our products and various other factors and uncertainties discussed in our filings with the U.S. Securities and Exchange Commission (the "SEC"). For a more detailed description of the risk factors and uncertainties affecting the company, refer to the Company's reports filed from time to time with the SEC, including the Company's Annual Report on Form 20-F. The forward-looking statements contained in this press release are made as of the date of this press release, and the Company undertakes no obligation to update or revise them, except as required by law.