NICE Actimize Releases 2022 Fraud Insights Report Identifying Threat Patterns Emerging Across Financial Institutions

Using anonymized data, insights were secured across online and offline payments channels, including P2P, ACH, wires, checks, and card transactions

Hoboken, N.J., May 16, 2022 – NICE Actimize, a NICE (NASDAQ: NICE) business, has released "The 2022 NICE Actimize Fraud Insights Report" that identifies and analyzes the leading fraud threats and patterns that impacted leading global financial institutions in 2021. Noting that banking fraud continues to rise, the data-driven research study found a 41% increase in attempted fraud over a similar evaluation conducted the year before by its data scientists.

Leveraging NICE Actimize's X-Sight AI, which utilizes Federated Learning techniques and collective intelligence to spot emerging threats and suspicious patterns of activity, the report was created by analyzing billions of banking and payments transactions representing over $110 trillion in value. NICE Actimize currently employs these techniques across leading financial institutions to monitor and stay aware of advancing fraud threats. Its data scientists and fraud subject matter experts compiled anonymized data secured from a subset of its total monitored transactions, including both online and offline payments channels that covered ACH, wires, checks, card purchases, and P2P transactions. The Fraud Insights Report aggregated and synthesized fraudulent activity patterns seen across a range of global financial institutions.

The NICE Actimize 2022 Fraud Insights report showed that increased utilization of mobile devices for everyday purposes, such as banking, shopping, and communication, heavily impacted the fraud landscape in 2021. Fraud increased across the board, from P2P payments and digital wallets to traditional check payments. Among NICE Actimize's findings, mobile channels saw the highest increase in fraud attempts. NICE Actimize projects that mobile channels will continue to be a target throughout 2022.

Additionally, the Fraud Insights Report's key findings also showed:

- Banking and payments transactions using mobile devices have increased substantially according to the report. But unfortunately, the popularity of mobile usage goes hand-in-hand with fraud – 61% of attempted fraud attacks through mobile apps are Account Takeovers (ATOs), the data showed.
- Fraudsters are exploiting the prevalence of mobile to target and leverage older devices. The report also showed that cell phones using older operating systems or made before 2016 have three times more fraud attempts associated with them than newer devices or operating systems.
- Nearly half (46.9%) of attempted fraud stemmed from card-not-present transactions across payment channels. As a result, online transactions presented a growing focus in the threat landscape.

Explains Craig Costigan, CEO, NICE Actimize, "Incidents of fraud against financial institutions and consumers continue to rise. For financial institutions to conquer these challenges, they must fully leverage data as the most important element of fraud prevention. World-class collective intelligence, with advanced analytics and AI, provides protections that safeguard banking channels while enabling more friction-free customer experiences."

NICE Actimize projects that P2P transactions will emerge as a dominant challenge impacting the 2022 threat landscape as financial institutions continue to see an acceleration of digital-initiated transactions. In its findings, NICE Actimize noted that P2P fraud saw an increase of 63% in attempted fraud dollar value and a 38% increase in attempted fraud rate in the past year.

To download a copy of NICE Actimize's 2022 Fraud Insights report, please click here.

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk, and compliance solutions for regional and global financial institutions and 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. In addition, 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. Find us at www.niceactimize.com, @NICE_Actimize or Nasdaq: NICE.

About NICE
With NICE (Nasdaq: NICE), it's never been easier for organizations of all sizes around the globe to create extraordinary customer experiences while meeting key business metrics. Featuring the world's #1 cloud-native customer experience platform, CXone, NICE is a worldwide leader in AI-powered self-service and agent-assisted CX software for the contact center – and beyond. Over 25,000 organizations in more than 150 countries, including over 85 of the Fortune 100 companies, partner with NICE to transform - and elevate - every customer interaction. www.nice.com.

Corporate Media Contact:
Cindy Morgan-Olson, +1 646 408 5896, NICE Actimize, cindy.morgan-olson@niceactimize.com, ET

Investors
Marty Cohen, +1 551 256 5354, ir@nice.com, ET
Omri Arens, +972 3 763 0127, ir@nice.com, CET

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 economic and business conditions, including as a result of the COVID-19 pandemic; competition; successful execution of the Company's growth strategy; success and growth of the Company's cloud Software-as-a-Service business; changes in technology and market requirements; decline in demand for the Company's products; inability to timely develop and introduce new technologies, products and applications; difficulties or delays in absorbing and integrating acquired operations, products, technologies and personnel; 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 breaches against the Company; 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.