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.

NICE · ACTIMIZE

Business Email Compromise

HALT BUSINESS EMAIL COMPROMISE ATTACKS

Business Email Compromise (BEC) is a social engineering attack in which fraudsters manipulate businesses and consumers into sending large sums of money via wire, ACH, BACs and other FI payment methods. BEC Losses have surpassed $3B in the U.S., according to the FBI -- and victims often experience high value losses.

While BEC attacks occur entirely outside the walls of the Financial Institution (FI), victims expect their banks to help them solve the problem. Predictive analytics can play a key role in detecting and stopping BEC attacks along with proactive customer education and the appropriate operational policies and procedures in place.

Fraud Solutions That Tackle BEC

- **Rich behavioral analytics:** Actimize solutions use behavioral analytics to develop customer profiles that define a baseline of normal user behavior, taking into consideration hundreds of factors, including unusual transaction amounts, new payees, and suspicious payee geography, for example.

- **Anomaly detection:** Actimize solutions use these rich customer profiles to spot suspicious behavior indicative of fraud in real time.

- **Anomaly detection and BEC:** Business Email Compromise is tricky because money movement is initiated by legitimate corporate customers. However, Actimize solutions catch these transactions because they are linked to behavior anomalies, such as suspicious payees, unusual or high focus payee geographies, unusual transaction amounts, etc.

- **Payment-specific scores with a wire focus:** Actimize offers payment-specific analytics, which detect anomalies that indicate wire fraud and result in high quality alerts. This is critical since wires are the primary target in BEC.

- **Self-development capabilities:** Actimize provides a self-development platform which allows users to develop complex analytics models specific to BEC and other emerging threats. These models can segment payment patterns and factors unique to BEC and wire fraud, considering complex payee information or unusual transaction cadence, for example.

- **Rules matter:** Actimize solutions allow FIs to write granular strategy rules to handle emerging threats and adapt quickly. In a Business Email Compromise scenario, an FI could identify corporate customers that have a higher likelihood to be attacked and then write risk rules to protect them. One of our customers calls this, identifying the “sloppiness level” of their corporate users.

- **Machine learning:** Actimize uses machine learning to uncover variables that can indicate previously unknown suspicious activity. We use this process to strengthen the quality of models and fraud risk scores. Actimize solutions include rapid response tools to modify models and secure tuning-on-demand.

- **Real-time decisions and challenges:** Actimize solutions make real-time decisions and challenges based on risk scores. This is especially important in BEC attacks where losses can be very high.

- **Operations and Investigations for BEC:** Actimize solutions allow users to prioritize BEC alerts and segment them into specialized workflows that assist investigators in navigating the challenging task of helping their clients identify BEC attacks.