A Growing Problem
PREVENT DATA BREACH FALLOUT
Fraudsters use these combinations of sensitive consumer data to commit Account Takeover (ATO), and to apply for credit cards, loans and new accounts.

Since the beginning of 2019:

- 120+ massive data breaches*
- 1.2 billion people affected by data breaches
- More than 5.5 billion U.S. bank account numbers exposed
- 1.1 billion pieces of PII exposed
- 4.8 billion Exposed PII results in wide scale ATO attacks—fraudsters have all the information they need to work the system and impersonate legitimate customers.

We continue to see a rise in different fraud schemes, directly linked to data breaches.

ATO and Third-Party Fraud: Exposed PII causes an uptick in synthetic identity fraud, or attacks where fraudsters use a combination of real and fabricated data to create new identities to open accounts or acquire loans.

Mule Accounts: Once fraudsters commit ATO, they need mule accounts to get money out of the system. Fraudsters also use the data from breaches to establish new accounts for mule purposes.

Synthetic Identity Fraud: Once fraudsters commit ATO, they need mule accounts to get money out of the system. Fraudsters also use the data from breaches to establish new accounts for mule purposes.

NICE Actimize’s Authentication-IQ solution uses expert-infused machine learning analytics, fueled by collective intelligence from our industry-wide view, to help FSOs detect ATO attacks in time to stop them.

In this era, where compromised PII is "the new normal," Financial Services Organizations need to rely on other data to identify their customers and protect their accounts.

The first step to detecting ATO begins at the point of login, where fraudsters fumble to get through authentication challenges. A risk-based authentication engine assesses the risk of login and authentication for every monetary and non-monetary transaction, using stronger authentication for riskier users. This is key to detecting and stopping ATO attacks, as well as preventing them from occurring in the first place.

FSOs can profile customers and related entities in real-time using historic transactions, geolocation, device, IP history, behavioral biometrics, authentication patterns, and much more across all channels to avoid relying on PII to identify a user. The more granular the profile, the more effectively you can use it for anomaly detection. Profiles should also dynamically update.

Fraudsters may use stolen data to take over accounts, but another way to keep fraudsters out of your system is by identifying behavior anomalies in real-time. Using machine learning and AI, a real-time detection engine will spot behavior anomalies—for example, unusual spending patterns or uncommon relationships—which enables FSOs to stop attacks.

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.

© Copyright 2023 Actimize Inc. All rights reserved.
info@niceactimize.com www.niceactimize.com/blog @nice_actimize

LinkedIn: linkedin.com/company/actimize
Facebook: facebook.com/NICEActimize

Learn more about Authentication-IQ