

PREVENT DATA BREACH FALLOUT

A Growing Problem

Data breaches are on the rise, affecting millions of people every year. Compromised data ranges from partial information, such as names and birth dates, to wider sets of personally identifiable information (PII).

Fraudsters use these combinations of

sensitive consumer data to commit Account Takeover (ATO), and to apply for credit cards, loans and new accounts.

the beginning of 2019: 1,2

Since

120+ massive data breaches*



people affected by data breaches

More than 5.5 billion

1.1 billion

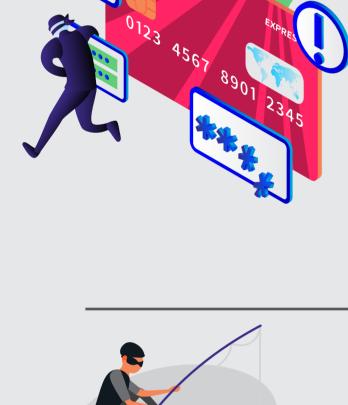
U.S. bank account numbers exposed



4.8 billion pieces of PII exposed

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

Data Breaches Feed



they need to work the system and impersonate legitimate customers.

Exposed PII results in wide scale ATO

ATO and Third-Party Fraud:

attacks—fraudsters have all the information

Synthetic Identity Fraud:

Exposed PII causes an uptick in synthetic

use a combination of real and fabricated

identity fraud, or attacks where fraudsters



accounts or acquire loans.

data to create new identities to open

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.

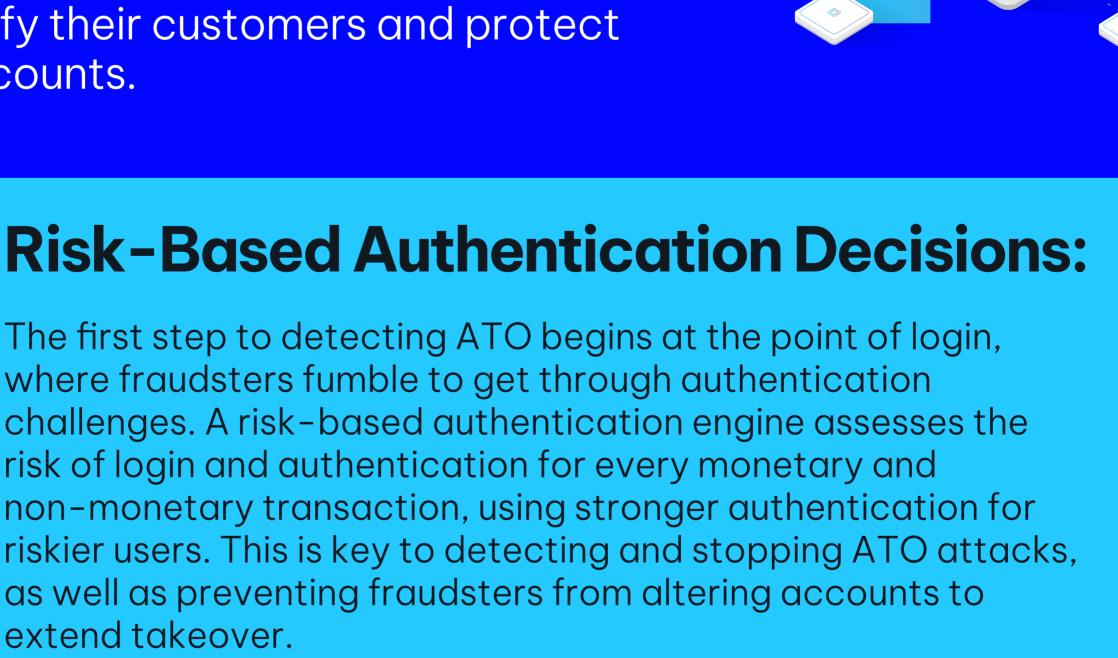
"the new normal," Financial Services Organizations need to rely on other data to identify their customers and protect their accounts. **Risk-Based Authentication Decisions:**

Omni-Channel ATO

In this era, where compromised PII is

Protection: Avoiding the

Fallout of Data Breaches





biometrics, authentication patterns, and much more across all

Entity Profiling:

extend takeover.

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. **Real-Time Detection:** Fraudsters may use stolen data to take over accounts, but

they can't successfully mimic customer behavior in a sustained

way. Using machine learning and AI, a real-time detection

engine will spot behavior anomalies—for example, unusual

FSOs can profile customers and related entities in real-time using

historic transactions, geolocation, device, IP history, behavioral



info@niceactimize.com

spending patterns or uncommon relationships—which enables FSOs to stop attacks.

FSOs detect ATO attacks in time to stop them.

https://www.comparitech.com/blog/information-security/biggest-data-breaches-in-history/

www.niceactimize.com/blog

NICE Actimize's Authentication-IQ solution uses expert-infused machine learning analytics, fueled by collective intelligence from our industry-wide view, to help

Learn more about Authentication-IQ

https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/\$FILE/ey-global-information-security-survey-2018-19.pdf 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

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.

Inkedin.com/company/actimize

consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time,

@nice_actimize

*Massive refers to data breaches impacting 10 million or more consumers 1. Albaugh, D. (2019, July 30). The Biggest Data Breaches in History. Retrieved August 7, 2019, from

2. Is cybersecurity about more than protection? EY Global Information Security Survey 2018-19. (2019). Retrieved August 7, 2019, from