
NICE
ACTIMIZE

# Combat the Big Business of Synthetic Identity Fraud

eBook

# Introduction

Fraud is a lucrative business that continuously adapts to the same market forces driving the behaviors of modern organizations. As the dynamics of the digital economy and virtual era evolve, the manifestations of application fraud are generating complex, quickly growing risks for financial services organizations (FSOs) and substantially influencing fraud control investment priorities.

# Identity-Related Crimes are on the Rise

NICE · ACTIMIZE

Fraud activity is expanding, influenced by economic and social disruption surrounding the COVID-19 pandemic, the massive shift to digital channels, and the rapid advancement of digitalization. Application fraud encompasses a diversity of criminal abuse of an account, and occurs when an account is opened and used to directly commit or indirectly support a criminal act.

**First-party fraud:** The account holder uses their account to defraud an institution.

**Mules:** Individuals who use accounts to knowingly or unknowingly traffic funds on behalf of criminals.

**Synthetic identity fraud:** The account holder uses an account to create and nurture a falsified identity to use for criminal activity.

# Trends & Drivers of Synthetic Identity Fraud

The dominant market trend toward identity-related crimes has been amplified by the environmental conditions of 2020. Attack pattern consistency indicates that synthetic identity fraud resulting from mule activity related losses as criminal behavior shifted toward creating and managing their own inventory in mule accounts.

NICE · ACTIMIZE

**13%**

of Mule Activity Resulting from Application Fraud

There are two primary types of synthetics:

- **Manipulated:** Specific attributes of an authentic identity are altered while retaining key data, such as the SSN or name. This is usually obtained from children, as they do not have a credit history and represent broad identity groups that are easy for fraudsters to hide within and difficult for FSOs to red flag or decline.
- **Manufactured:** An identity is patched together using real attributes from multiple identities, or all attributes are completely falsified. These are typically difficult to authenticate, and proliferate once the identity enters an FSO and matures.

NICE · ACTIMIZE

Synthetic identities represent 52% of application fraud

# All Fraud is Not Created Equal

Market trends are triggering FSOs to strengthen control frameworks so they can distinguish legitimate identities accurately and intelligently from synthetic or stolen identities. As synthetic identity fraud is more challenging to detect, it requires a powerful strategy and sufficient coverage against all forms of application fraud.

Leading fraud practitioners are quantifying associated risks throughout the entire customer lifecycle to establish a foundation for granularly managing customer profitability and automating controls around legitimate and synthetic identities. This simultaneously drives potential for service delivery differentiation and customization, which are key pillars in providing a competitive, meaningful customer experience.

NICE · ACTIMIZE

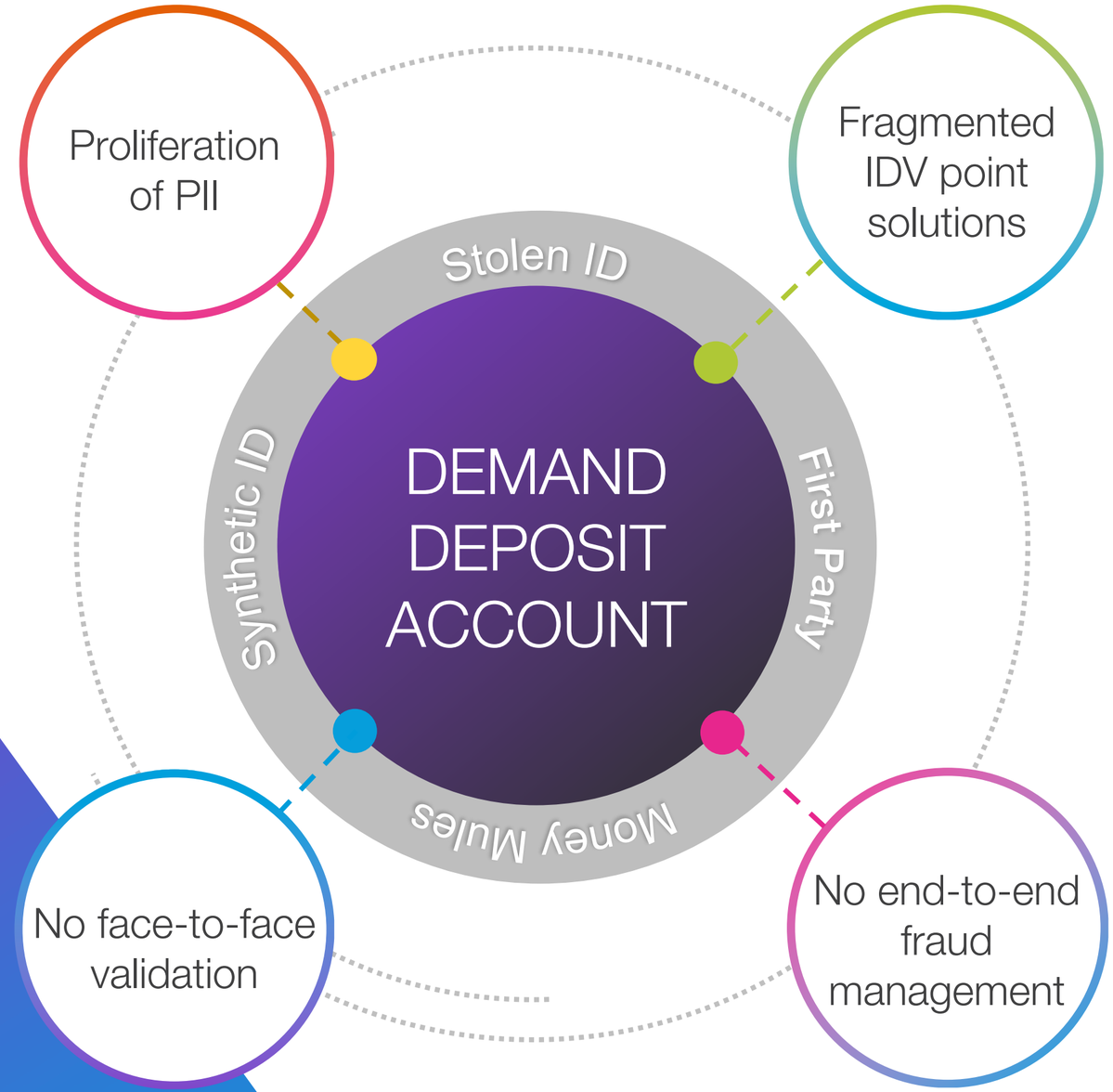
# The Fraud-Accessible Enterprise Climate

Synthetic identity fraud is not limited to a specific transaction or typology, but rather includes any fraud manifesting from a synthetic or stolen identity across all payment channels and transactions. DDA accounts represent one of the simplest vehicles for criminals to enter an FSO, mature an identity, spread to different product lines or loan accounts, and ultimately defraud the organization.

## The main enablers of this scenario include:

- Availability of personally identifiable information (PII) on the dark web.
- Lack of a central source of truth for identity verification.
- Data silos and segmentation that create a disconnect between the application and transaction processes.
- Ease of breathing life into a synthetic identity by creating a file on a credit bureau to enhance validity.
- Inaccurate identity data across data sources, leading to more common red flags.

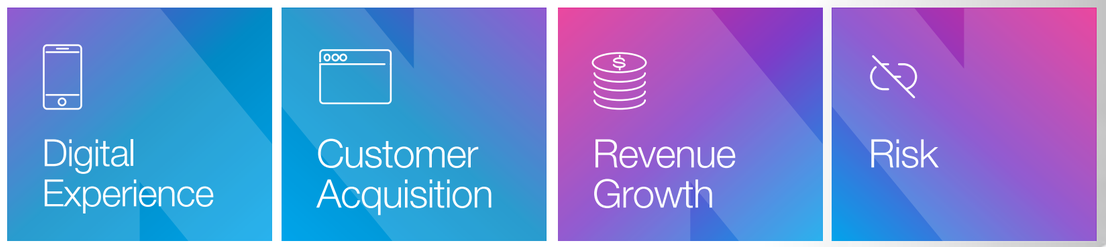
Application fraud losses for DDA application fraud projected to hit US$939 million in 2023.[1]




NICE · ACTIMIZE

# Balancing the Scales Between Growth & Risk

FSOs have accelerated their digital transformation, eliminating the need to for face-to-face account opening and creating a climate easily susceptible to synthetic identity fraud.




Fraud prevention professionals must lead their organizations in the journey to provide the optimal level of friction that drives safe account growth.

NICE · ACTIMIZE

"Risk management has not kept pace with the proliferation of digital and analytics transformations — a gap is opening that can only be closed by risk innovation at scale."

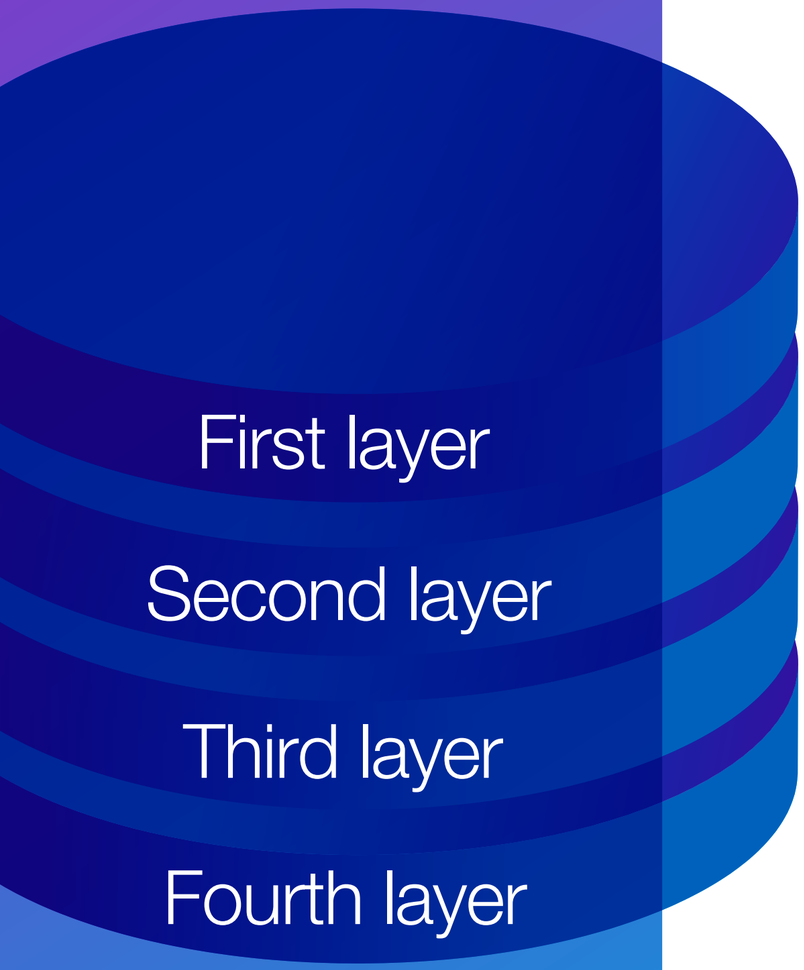
*McKinsey & Company Derisking Digital and Analytics Transformations, January 2021*

NICE · ACTIMIZE

# Closing the Gateway to Fraud with a Multi-Layered Defense

FSOs need a multi-layered solution and defense strategy to enable accurate identity assessments, detect abnormal or suspicious transaction behaviors, and execute dynamic fraud prevention from the initial onboarding event to ongoing enterprise fraud monitoring.

The considerable pressure to support revenue growth objectives by way of optimizing new client acquisitions is a motivating force for strengthening the layers of identity verification controls.[1]




Protect the customer origination gateway by correlating real world and digital identity data to substantiate that a presented identity is legitimate.

Perform identity proofing and corroboration that extends from account origination through the customer transaction journey.

Connect the various attributes of each layer to ongoing fraud monitoring capabilities to better determine synthetic or stolen identities hidden within the existing portfolio.

Segment applications into journeys with friction that corresponds to the risk.

NICE · ACTIMIZE

# Stop Synthetic Identity Fraud with End to End Fraud Prevention

IFM-X's New Account Fraud provides identity intelligence enriched with behavioral and transactional analytics to optimize risk detection during discrete phases across the customer lifecycle - from origination to early account and ongoing monitoring.

IFM-X

- Multi-layered solution using advanced AI and machine learning
- Dedicated analytics to cover identity and first-party fraud risk in digital origination channels
- Orchestration and corroboration of identity data for precise identity risk matrix
- Early account monitoring to identify fraudulent accounts and stop fraud losses
- Holistic view of customer risk: identity, accounts, transactions and risk
- Entity-level view of identity and first-party fraud risk

NICE · ACTIMIZE

Detect and defend against synthetic and stolen identity fraud with the power and intelligence of AI throughout identity verification, holistic early monitoring and throughout the customer lifecycle across all channels.

Learn More

[1] Aite Group LLC, Application Fraud: Accelerating Attacks and Compelling Investment Opportunities, November 2020

## 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.

© Copyright 2021 Actimize Inc. All rights reserved.

www.niceactimize.com