NICE
ACTIMIZE

3 Ways to Prevent New Account Fraud

Traditional fraud prevention cannot successfully detect and defend against fraudsters using complex frauds manifested from synthetic and stolen IDs. Instead, it leaves the gate unlocked for professional fraud gangs.

eBook

New Account Fraud Defined

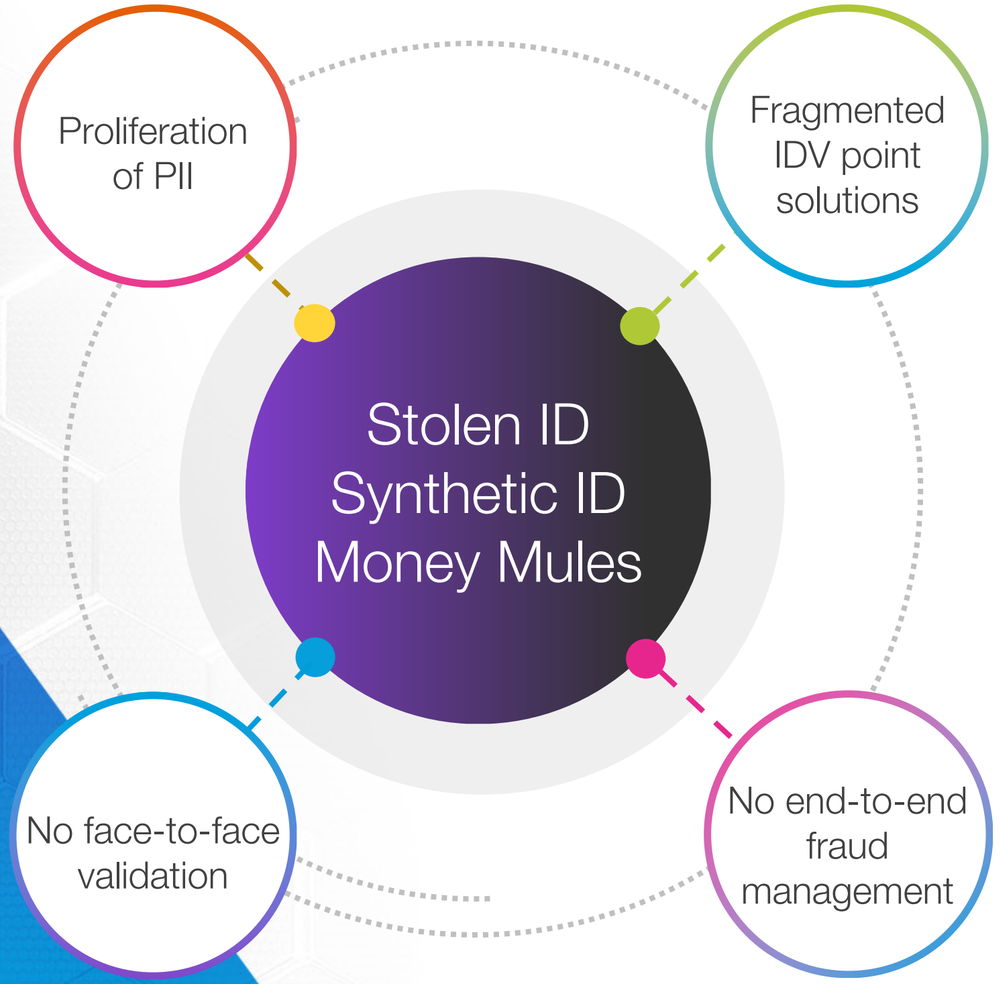
New • Account • Fraud | n. 1. the act of opening an account with the intent of criminal activity or fraud.

Recent market events coupled with fragmented and siloed fraud prevention technologies make financial services organizations vulnerable to complex and organized fraud – **estimated at $1 billion in losses by 2023 for direct deposit accounts alone.**[1]

NICE · ACTIMIZE

The explosion of Personally Identifiable Information (PII) on the dark web has helped drive sophisticated fraud schemes that use stolen and synthetic identification.

As consumers demand accelerated digital options when managing their money or shopping online, this fraud challenge will only get worse.



Orchestrating and Connecting the Ecosystem

Most organizations continue to treat account application review processes and account monitoring separately.

Bringing together identity and authentication along with AML and Fraud profiling leads to lower risk, better conversion and improved profitability.

Fraudsters know this and look at the debit deposit account (DDA) digital application process as the easiest method to get into the organization using a stolen or synthetic identity. They can then later use the account for fraudulent activity potential en masse.

To protect from stolen and synthetic IDs, fraud teams need to:

- Orchestrate identity verification (IDV) data and point solutions
- Use advanced AI as an intelligent layer on top of the IDV data to provide powerful analytics and risk profiling
- Connect application and identity risk data to early account monitoring

New Account Fraud doesn't just stop at new account decision.

85% *to* 95% *of synthetic identities are not caught by the existing fraud model.*[2]

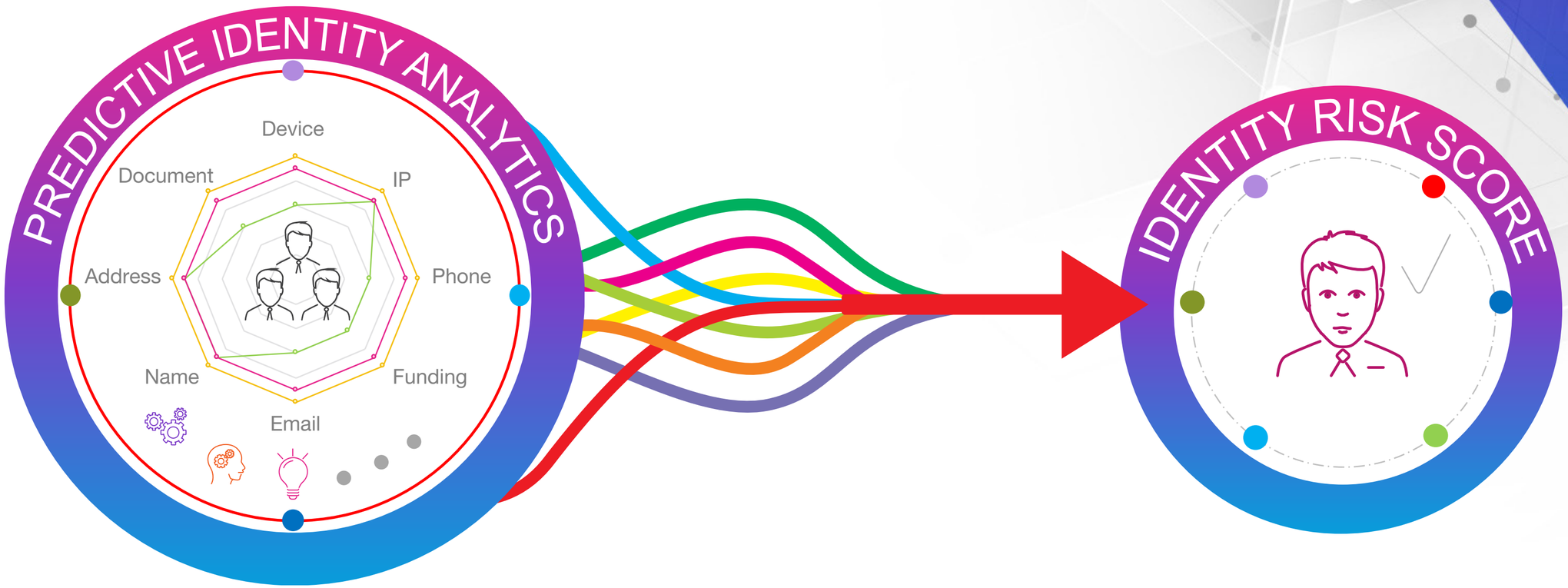
NICE · ACTIMIZE

Consider taking a holistic approach, removing silos and having the option to reuse services throughout the customer lifecycle

1 Prevent New Account Fraud with Identity Proofing

NICE · ACTIMIZE

Safely drive account growth across all digital channels



Using advanced AI to add a layer of intelligence across all IDV point solutions and thousands of data points will provide a single precise identity risk score.

Successfully deploying intelligent identity proofing provides:

- Lower false positive rejections
- Less fraudulent accounts opened
- Reduced friction and application abandonment
- Risk score for use in early account monitoring

Move away from Accept/Decline to a more granular risk model.

Model your credit losses for fraud and break them out into first-party fraud, synthetic and identity theft.

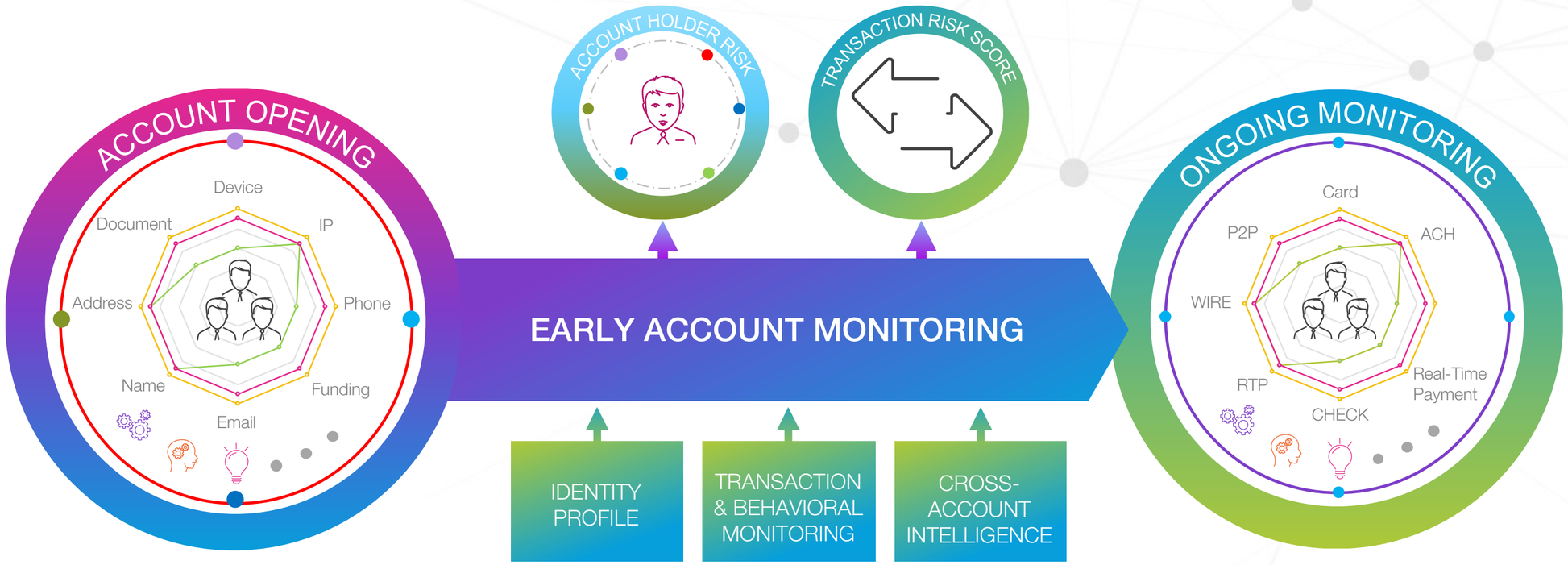
Taking this approach also allows for improved propositions such as:

- Immediate account opening and funding
- Instant overdrafts
- Instant enrollment to:
  - Request for Payment
  - Mobile Remote Deposit Complete (mRDC)
  - App
  - Zelle
- Real-time payment limits
- New beneficiaries

2 Prevent New Account Fraud with Early Monitoring

NICE · ACTIMIZE

Use intelligent and dynamic risk profiling to optimize account access and growth potential



NICE · ACTIMIZE

Move away from check once and forget, and instead use ongoing risk assessments for a multitude of risks:


AML


Fraud


Credit

High accuracy early monitoring using application data and identity risk scores provides:


Dynamic account access and limits


Detects and defends new account fraud

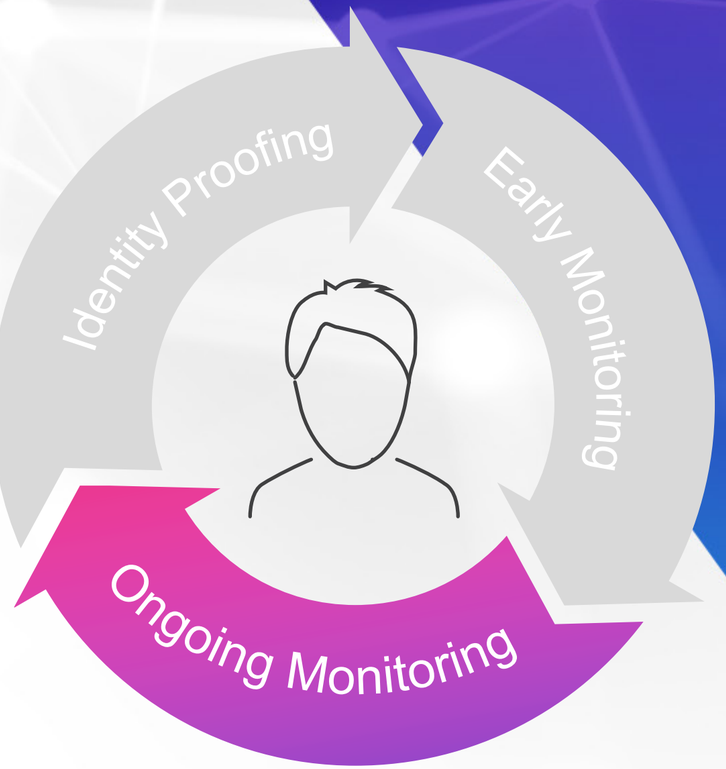

Establishes baseline profiles

3 Prevent New Account Fraud with Optimized Ongoing Monitoring

NICE · ACTIMIZE

Connecting data across the entire customer lifecycle

Traditional transaction-based fraud prevention solutions take up to 90 days to accumulate enough data for their AI/ML models to be effective. By starting fraud prevention coverage earlier and breaking down data silos, the time to value for transaction monitoring is compressed to remove the cracks that fraudsters can exploit.



When it comes to ongoing monitoring, one size doesn't fit all.

Investment in the ecosystem and orchestration will allow risk-based service provision products to work throughout the lifecycle.

This will improve detection of:

Mules

Account takeover

New account fraud

Optimal fraud prevention must be holistic, with the ability to stream data in real time to detect and defend against emerging threats. This includes:

Seamless connection of data from early account history

Immediate transaction protection

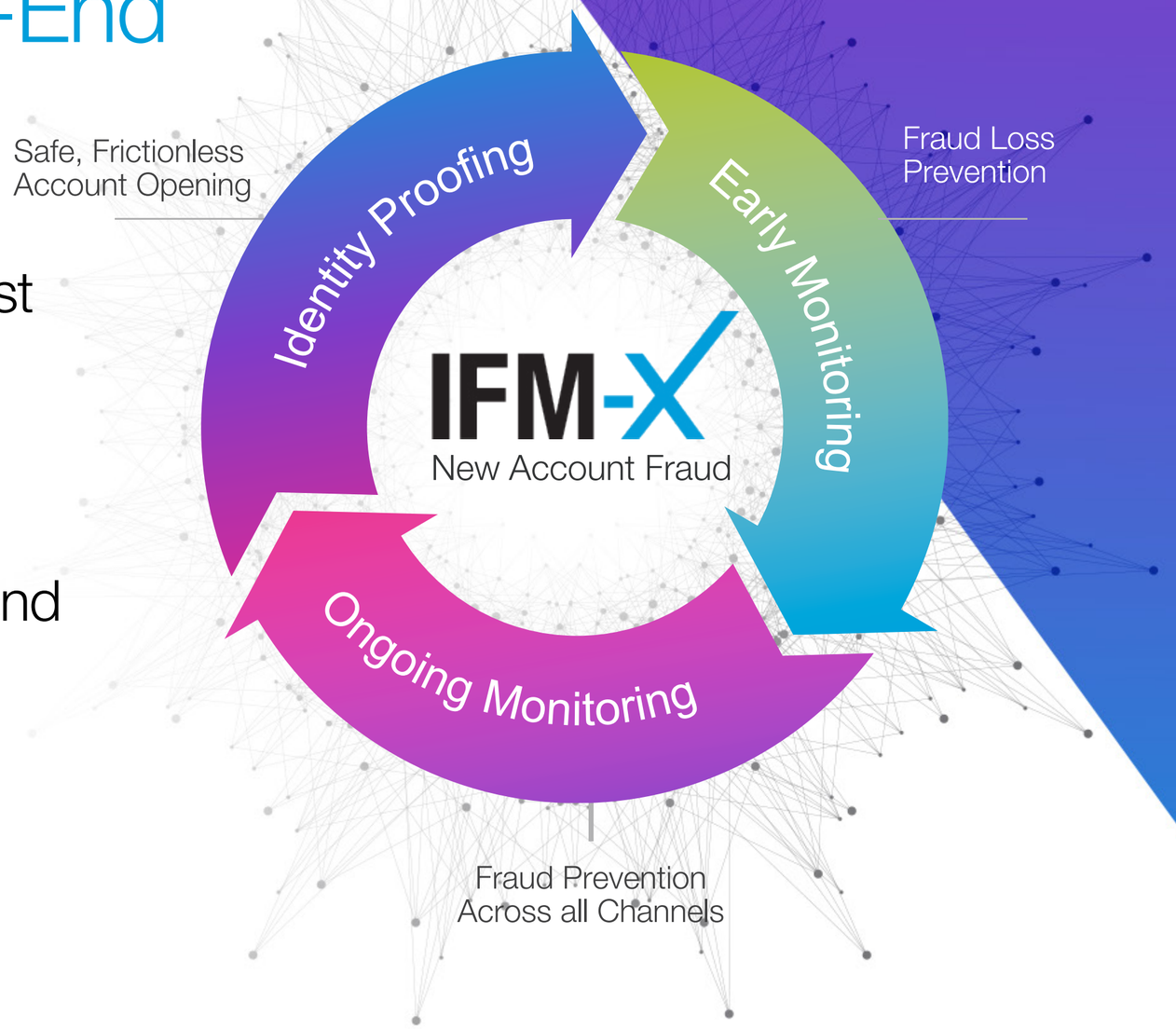
Reduced false positives and higher value detection rates

Verify, Monitor and Trust All New Accounts with End-to-End Fraud Prevention

NICE · ACTIMIZE

Fraud schemes and mule activity that manifest from stolen or synthetic IDs are exceedingly difficult to detect at initial application.

Start fraud oversight earlier in the account lifecycle to provide comprehensive, end-to-end protection that continually analyzes account activities, identifies risk and monitors transactions.



NICE · ACTIMIZE

TOPLINE | Reduced friction leading to lower abandonment rates and application rejection rates to drive new account growth through digital channels.

OPERATIONAL | Orchestrate, connect and enhance your ecosystem of data and point solutions for IDV and fraud management.

BOTTOMLINE | Reduce direct fraud loss as well as prevent downstream fraud loss across the organization.

Fight new account fraud now

Download Brochure

[1] Fooshée, T. (n.d.). Application Fraud: Accelerating Attacks and Compelling Investment Opportunities (2020 ed., Vol. November, Rep.). Aite Group.

[2] Synthetic Identity Fraud in the U.S. Payment System A Review of Causes and Contributing Factors, fedpaymentsimprovement.org

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.

www.niceactimize.com