DEDUCE

SOLUTION BRIEF

Stolen and Synthetic Identity Fraud Prevention Has a Trust Problem

AUGUST 2024

INDUSTRIES: All

Multicontextual Identity Intelligence at Scale Provides the Solution

> *Legacy approaches to AI-driven identity fraud increase friction, false declines, and costs without stopping fraud.*

The AI Revolution Cuts Both Ways

AI and automation are accelerating creativity and efficiency across industries—including organized identity fraud. For example, fraudsters can leverage AI with stolen PII to:

- Cheaply synthesize and orchestrate batches of credible digital identities.
- Authenticate those identities with AI-generated ID documents, biometrics, and even deepfake voice and video impersonation.
- Create credit histories via low-cost automated actions such as prepaid card and phone transactions.
- "Pig butcher" a credit score by repaying small subprime loans.
- Create online histories using "aged" and geolocated email addresses, merchant account creation, and engagement with brands.

The result is a virtual army of stolen and synthetic identities that are indistinguishable from legitimate identities.

Each of these AI-driven identities can pass automated fraud controls, IDV assessments, manual reviews, and virtual risk analysis assessments for documentation, 2FA, account age, and credit history.

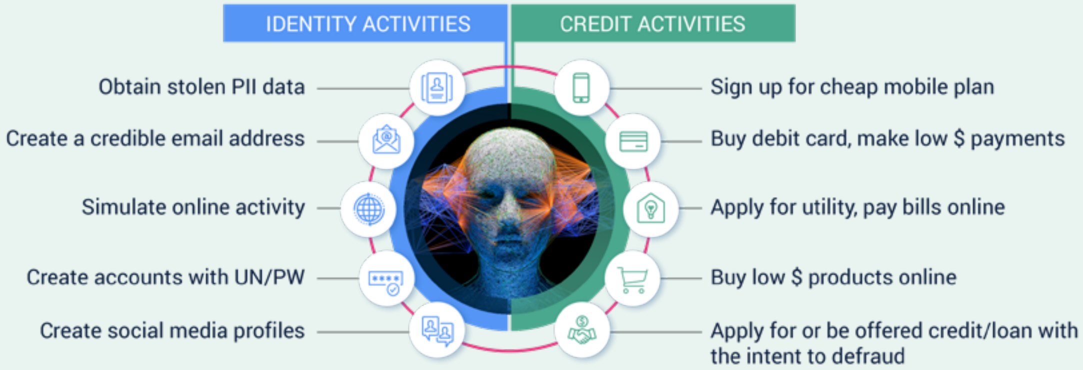
> ***Financial institutions fail to detect an estimated 95% of synthetic identities during onboarding.***[1]

AI-enabled identity fraud at scale has the potential to hit businesses with waves of fraud that cause financial losses, more onboarding friction, more frequent false positives, higher customer acquisition costs, and poor performance on other customer acquisition KPIs.

Existing Fraud Prevention Solutions Can't Detect AI–Driven Threats

Today's fraud solutions may be good at spotting traditional identity fraud in specific contexts, but they were created before generative AI changed the fraud game. As a result, traditional fraud detection:

- Draws on narrow data sources to assess an individual email address or phone number, with no context about its relationship to other identities.
- Uses static data and prescriptive algorithms that prevent a full contextual view of the identity's behavior over time, which can lead to missed fraud indicators.
- Relies on databases that only look at identity behavior in one context, like online shopping or banking, for an incomplete view of activity.


IDENTITY ACTIVITIES
CREDIT ACTIVITIES
Obtain stolen PII data
Create a credible email address
Simulate online activity
Create accounts with UN/PW
Create social media profiles
Sign up for cheap mobile plan
Buy debit card, make low $ payments
Apply for utility, pay bills online
Buy low $ products online
Apply for or be offered credit/loan with the intent to defraud

Signature activity pattern of stolen and synthetic identities

- Cannot recognize the patterns and digital fingerprints associated with AI-driven identity fraud.
- Lacks the scalability to identify and counter AI-generated fraud attacks.
- Relies too much on behavioral biometric or device-centric fraud solutions that AI deepfakes and SIM swaps can defeat.

Because of these factors, current fraud solutions can't distinguish an AI-generated stolen or synthetic identity from a real one. Even fraud prevention escalation policies such as manual reviews and KYC requirements will not catch these very sophisticated identities, and doubling down on those strategies can increase costs, approval delays, and false positives. After approval, AI-driven stolen and synthetic identities act as "sleepers," waiting for an offer of credit that they can exploit—and then they disappear.

> *"Financial institutions are finding that as much as 30% of their bad debt is actually fraud. These debts are uncollectible because the borrowers, to whom they issued credit, never intended to pay and may have been nothing more than synthetic identities."*
>
> **- FICO**

Using Identity Intelligence to Stop Stolen and Synthetic Identity Fraud

Detecting AI-driven stolen and synthetic identities requires identity intelligence at scale—over time and mapped to geographies and device networks—to evaluate each identity against other identities in as many digital contexts as possible.

Only multicontextual identity intelligence at scale can:

- Gather and analyze extensive real-time activity-backed identity data from diverse sources.
- Work with ML to recognize the activity patterns and digital fingerprints created by AI-generated fraud.
- Identify activity matches between the identity under review and other identities.

Multicontextual identity intelligence at scale also:

- Detects traditional identity fraud accurately and precisely.
- Reduces false positives and minimizes manual review requirements.
- Restores the reliability of customer onboarding practices.
- Identifies new threats as they emerge.

Protect Your Business from Stolen and Synthetic Identity Fraud

Contact us for an evaluation of your new account opening workflow and guidance on how to identify stolen and synthetic identities, protect your new customer experience, and restore trust in your onboarding process.

[1] Thomson Reuters, **Trends in synthetic identity fraud**