HELP GUIDE

Advice to Detect & Mitigate

# SYNTHETIC FRAUD

AUTHENTICID

## Synthetic Identity Fraud Explained.

Synthetic Identity Fraud (SIF) is a complex form of identity theft that occurs when a fraudster uses a combination of personally identifiable information (PII) of individual(s) to create a false or "synthetic" identity. This identity is used to commit a dishonest act for personal or financial gain. Synthetic Identity Fraud is fast-growing and is notoriously difficult to detect due to it's complexity, and the rise in "faceless" online transactions.

**A 48 BILLION DOLLAR PROBLEM**

Synthetic Fraud is expected to drive $48 billion in annual online fraud loss.

*Online Payment Fraud Report, Juniper Research 2022

*The Two Categories of Synthetic Identity Fraud to Watch For:*

- **Manipulated Synthetic Identities:** This is when a person slightly modifies real PII, typically their own, to create a new identity, as a means to hide bad credit.
- **Manufactured Synthetic Identities:** This is when a fraudster steals PII, often sold on the dark web, and combines that PII with other stolen identity data of another individual, or fake PII.

## How Fraudsters Wreak Havoc with Synthetic IDs

Often a first step a fraudster takes with their new synthetic Identity is to apply for credit, then make small purchases that proceed timely payments. Once good credit history is obtained they purchase big ticket items, get a loan, attain government benefits and then... disappear into thin air.

## A Growing Threat that Impacts Businesses and Individuals

Synthetic Fraud causes problems for just about everyone:  financial institutions, government, merchants, and the victims whose identities has been compromised.

After a synthetic identity is created, the owner of the legitimate Social Security number is responsible for any debts or liabilities associated with the fraud that has been perpetuated.

Banks and payment processors that fall victim to synthetic fraud incur major losses and as a result are forced to raise prices and interest rates to ensure profitability.

Retailers and eCommerce merchants pay a hefty price when it comes to synthetic fraud. They lose out on merchandise costs, shipping costs, administrative costs, and incur chargebacks when fraudsters use synthetic IDs to buy products and falsely claim they didn't make the purchase for a refund.

- ✓ Credit Card Fraud
- ✓ Car Loans Scams
- ✓ Telecom & Utility Scams
- ✓ Tax Return Scams
- ✓ Unemployment Scams
- ✓ Social Security Scams

## Steps for Mitigating Synthetic Fraud

1. Conduct internal evaluations to understand potential risks, points of failures, and important benchmarks.

2. Increase onboarding requirements, with advanced screening procedures that follow today's best practices and take a multi-layered approach to fraud detection.

3. Strive for a holistic customer view, that aggregates data from multiple channels.

4. Adopt technology that detects, alerts and mitigates fraud activity and data inconsistencies. Machine learning and AI driven technology, will enable superior results over human identity verification.

5. Continuous audit systems and process on a regular cadence to ensure  things are running properly and fakes and red flags are being detected.

AUTHENTICID

# Good vs.Bad Detection Signals

To combat synthetic identity fraud, it's imperative to know the signs. A reliable way to detect fraudsters is through a holistic view of a broad data set to identity anomalies or inconsistencies in an identity record.

## ✗ Red Flags

- Multiple authorized users on the same account. Fraudsters will "piggyback" and add their synthetic ID unknowingly to valid credit acounts
- Recently issued Social Security Number's - it's common for frausters to hijack a child's SSN
- SSN# that matches a different consumer profile
- Credit depth that does not match customer profiles
- All new data entities e.g. Address, Profile Image, and email address
- Multiple accounts from one IP Address
- Using unsecure credit to build history

## ✓ Good Signs

- High quantity of data associated with an identity
- Social media accounts with history, activity and connections
- Online and offline data points that connect
- Multiple physical addresses with unique time stamps
- Emails associated with non-free accounts

## How AuthenticID Identity Proofing Technology Can Help:

### ID Verification

Verify government-issued IDs in seconds with 99%+ accuracy. Detects fraudulent documents with more than 2,000 unique computer vision data models.

### Biometric Authentication

Confirm a person's true identity with just a selfie. Our facial recognition software leverages proprietary AI and Machine Learning to verify an identity and Face-Match the selfie to another photo.

### Fraud Shield

Block fraudsters indefinitely. Fraud Shield allows you to identify, flag and add users to the Bad Actor Watchlist using biometric and biographic data.

### Liveness Detection

Ensure the person taking a selfie to verify their identity is actually present. Liveness detection stops the most sophisticated spoofing including face masks & deep fakes.

Learn more at www.authenticid.com