

# 1Kosmos Synthetic ID Fraud Prevention

Verify identity anywhere, anytime with over 99% accuracy to eliminate synthetic ID fraud.

## A Growing Threat that Impacts Both Businesses and Individuals

### The Business Challenge

Organizations offering access to online services are facing a new challenge - Synthetic Identities.

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 its complexity, and the rise in "face-less" online transactions.

The ID Analytics study states that synthetic identity fraud currently accounts for 80 -85 percent of all identity fraud and results in billions of dollars of damage worldwide - making it one of the fastest growing types of identity fraud.

To mitigate the threat, organizations must rethink how they currently enroll and verify identities remotely. They need to digitally verify and secure identities at scale and in doing so modernize traditional IAM and CIAM strategies. We have always needed to verify identities, but the need for automated digital identity-proofing has become clear in today's shift to a digital-first expectation and the explosion of online identity fraud. This shift requires users to prove who they are with more than a username, a password, and a one-time code.

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

To mitigate the threat, organizations must rethink how they currently enroll and verify identities remotely. They need to digitally verify and secure identities at scale and in doing so modernize traditional IAM and CIAM strategies.



## The 1Kosmos Identity Proofing Advantage

Recognizing the need for accurate identity onboarding and secure access, the 1Kosmos platform is built to detect synthetic identities and reduce new account fraud. The two categories of synthetic identities that 1Kosmos can prevent are:

### **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.

1Kosmos is certified to the NIST 800-63-3 guidelines and automatically supports remote self-service enrollment to Identity Assurance Level 2 (IAL2) or higher with agent assistance.

1Kosmos is also a certified AAL2 FIDO2 biometric authenticator and stores customer information in a distributed ledger to W3C DID standards to ensure the very highest level of privacy.

1Kosmos identity proofing utilizes a user's driver's license, passport, or National ID to validate user identity. With the user's consent, 1Kosmos then extracts content from the ID and verifies the document's validity. 1Kosmos supports document verification for over 150 countries. The extracted data, including the picture, is used to verify the user's identity and is encrypted with the user's private key and stored in the 1Kosmos private and permissioned blockchain protecting data and privacy.

Once enrolled, the user can prevent account takeover by using their identity for passwordless access during account login and for transaction approval.



# 1Kosmos Synthetic ID Fraud Prevention

## New Customer or Citizen Onboarding

1Kosmos binds the user to a verified and validated identity.

Our solution provides organizations the ability to complete a mobile-first onboarding journey for workforce, customers, or citizens. Once a user begins their account setup, a process starts to verify the new identity remotely leveraging the #1 algorithm rated by NIST for non-biased decisioning.

Depending on the level of assurance required, the user will be guided to enroll their identity. For those instances where high identity proofing assurance is required, the user must enroll one or more forms of government-issued ID. The captured data is encrypted with the user's private key and goes through another level of encryption before being stored in the 1Kosmos private and permissioned blockchain.

The process of validating and verifying the identity prevents synthetic ID fraud. At the same time, the user account is generated and enrolled in an enjoyable passwordless experience.

## Government Issued IDs

1Kosmos identity proofing will utilize a user's driver's license, passport, or National ID to validate a user's identity.

With the user's consent, 1Kosmos extracts the content from the ID and verifies the document's validity. 1Kosmos supports document verification for over 150 countries. The extracted data, including the picture, is used to verify the user's identity and is encrypted with the user's private key and stored in the 1Kosmos private and permissioned blockchain protecting the user's data, privacy and eliminating synthetic ID fraud.

As Government-issued IDs are updated, users can delete their expired ID and enroll the new ID.

## Our identity proofing technology can:

- Read barcodes defined by PDF 417 standard that has data encapsulated in it
- Read the data stored in an MRZ code on both passports and National ID's
- Read and extract the secure data located in passport RFID chips
- Communicate with issuing authorities to verify data accuracy
- Identify fraudulent IDs during time of capture



---

## Document Verification

Identity proofing is only as sound as the ID used. 1Kosmos identity proofing technology captures the information in the ID and looks to ensure the ID is valid.

For instance, 1Kosmos checks for common characteristics of the entered document to identify if a photocopy is used. The RFID chip in a passport is another example, where if the chip can not be read, then the data is not validated.

In cases where a visual check of the data is required, 1Kosmos will work with third parties to validate the captured data and the ID document. Or, if organizations would prefer, 1Kosmos can activate an API to verify the data from the Country Signer Certificate Authority (CSCA) or from an issuing authority, such as AAMVA for US drivers licenses, to validate the document and the data.

## Driver's License

To validate the driver's license, the user is instructed to put the ID on a flat surface with a darker background so that 1Kosmos can easily detect the contrast between the back and front of the driver's license.

This also helps detect fraudulent documents or documents that are printed on a piece of paper. 1Kosmos compares the data extracted from the back of the driver's license PDF 417 with the data captured from the OCR scan of the front to validate the data, and the picture captured is used to validate the LiveID biometric scan.

All of the data is encrypted with the user's private key and stored in the 1Kosmos private and permissioned blockchain and can be shared at the user's discretion if requested.

## Passport

1Kosmos can verify identity through three areas of the passport to validate the data and document.

First, an OCR scan of the passport data page is done, with all of the information in a human-readable format. Second, 1Kosmos reads and captures the MRZ code containing an encoded version of the identity data. And Finally, 1Kosmos can read and compare the data on the NFC chip if the mobile device supports NFC and this level of verification is needed.

These three data points will triangulate all of the identity data that increases the identity assurance level of the user. All of the data is encrypted with the user's private key and stored in the 1Kosmos private and permissioned blockchain and can be shared at the user's discretion if requested.



## Identity Proofing SDK

Our identity proofing functionality is available through our SDK and is easily integrated into any custom app. So no matter if you are using the 1Kosmos app or a custom integration, you can implement a mobile-first automated identity proofing workflow.

## Compliance

1Kosmos is certified (by the Kantara Initiative) to NIST Identity Assurance Level 2 and compliant with Identity Assurance 3, as per the NIST 800-63-3 digital identity guidelines.

Level 3

Level 2





## About 1Kosmos

1Kosmos enables remote identity verification and passwordless multi-factor authentication for workers, customers and residents to securely transact with digital services. By unifying identity proofing, credential verification and strong authentication, the 1Kosmos platform prevents identity impersonation, account takeover and fraud while delivering frictionless user experiences and preserving the privacy of users' personal information. 1Kosmos performs millions of authentications daily for government agencies and some of the largest banks, telecommunications, higher education, and healthcare organizations in the world.