USE CASE: IDENTITY VERIFICATION SOLUTION

INTRODUCTION

Machine learning models can detect synthetic identities in real time during onboarding. The following case study illustrates how these models can detect synthetic identities and determine if a fraud ring is involved.

CASE STUDY

An application is submitted to an online lender with the following identity data. While not shared on the application, the IP address (internet protocol address that identifies the device on the internet or a local network) also is collected at time of submission.

APPLICANT		
NAME: Joe Smith	**DOB:** 03/31/1957	**SSN:** 007-44-1776
IP ADDRESS: 00.00.00.111	**EMAIL ADDRESS:** joe@email.com	**PHONE NUMBER:** 555-555-1212
ADDRESS: 44 Saint Marks Place, New York, NY 10003		

Most synthetic identity fraud solution providers are connected to a bank's onboarding platform via an API (application programming interface), so applicant data can be sent as it streams in. When application data is received, it is compared with previous applications, as well as third-party identity data that is pulled together in house. The application data is compared to known fraudulent identities, evaluated for red flags and put through models to be scored along multiple dimensions. This is generally done in less than a second to not slow down the overall application process.

Each solution provider's score varies. In this example, the provider's score range is from 0-999. The higher the score, the higher the risk.

USE CASE: IDENTITY VERIFICATION SOLUTION

In the case of Joe Smith, this identity scored 916 and is considered a very high risk for synthetic identity fraud. The risks detected with this identity include:

- **Social Security number (SSN)** was issued in 2008 in California, but the date of birth is 1954 and current address is in New York. There are exceptions, but most Americans are issued an SSN in their birth year and state. Data related to the date and state of issuance of SSNs often is incorporated into models, so an SSN provided can be evaluated to determine if it makes sense given the date of birth and address supplied.

- **Home address** has been used in the past by known criminals. When specific addresses are used repeatedly by fraudsters, they get added to an "address negative list." In this case, the address is on the negative list because it is known to be used by fraudsters.

- **IP address** is far from the applicant's street address. Fraud rings often submit applications from one location, which may be outside the United States. A synthetic fraud model often determines the location of the IP address to discern its distance from the street address.

- **Email address** has never before been seen in a credit application. New email addresses often are associated with synthetic identities.

Not only has the technology determined this is likely a synthetic identity, but clustering technology also indicates the identity is part of a fraud ring.

CLUSTERING

Fraud rings can be detected in real time by linking together matching identity data across hundreds of millions of identities. A simple example on the next page illustrates three other applications showing an SSN with the same first five digits and same last name. The SSNs for all four people were issued on the same date and in the same state. The "first seen" date, or the date when the SSN initially was used to apply for credit, also is the same for all four identities. All four identities are associated with the same negative list address. This indicates a high likelihood that all four applications are part of the same fraud ring.

USE CASE: IDENTITY VERIFICATION SOLUTION

IDENTITIES			
NAME: Joe Smith	**DOB:** 03/31/1957	**SSN:** 007-44-1776 **ISSUED:** 2008 CA **FIRST SEEN:** 10/01/2018 **LAST SEEN:** 09/01/2021	**ADDRESS:** 44 Saint Marks Place, New York, NY 10003 **FIRST SEEN:** 10/01/2018 **LAST SEEN:** 06/10/2021
NAME: Joel Smith	**DOB:** 03/18/1962	**SSN:** 007-44-1990 **ISSUED:** 2008 CA **FIRST SEEN:** 10/01/2018 **LAST SEEN:** 09/01/2021	**ADDRESS:** 44 Saint Marks Place, New York, NY 10003 **FIRST SEEN:** 10/01/2018 **LAST SEEN:** 06/10/2021
NAME: Alex Smith	**DOB:** 07/25/1959	**SSN:** 007-44-2026 **ISSUED:** 2008 CA **FIRST SEEN:** 10/01/2018 **LAST SEEN:** 09/01/2021	**ADDRESS:** 44 Saint Marks Place, New York, NY 10003 **FIRST SEEN:** 10/01/2018 **LAST SEEN:** 06/10/2021
NAME: Alexander Smith	**DOB:** 10/01/1971	**SSN:** 007-44-1800 **ISSUED:** 2008 CA **FIRST SEEN:** 10/01/2018 **LAST SEEN:** 09/01/2021	**ADDRESS:** 44 Saint Marks Place, New York, NY 10003 **FIRST SEEN:** 10/01/2018 **LAST SEEN:** 06/10/2021

The identity verification solution quickly assessed the applicant's risk to enable the financial institution to make a decision about how to proceed with the application. The solution analyzed large amounts of data very quickly to identify a potential synthetic identity without creating friction that could negatively impact legitimate applicants.