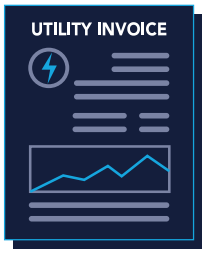
COMBATTING FRAUD WITH A SUITE OF IDENTITY VALIDATION TOOLS

As part of the Know Your Customer (KYC) process, current Customer Identification Program (CIP) regulations require financial institutions to verify the identity of an individual seeking to use their services. At a minimum, they must verify the customer's name, date of birth, address and identification number (e.g., a Social Security number). Customer Due Diligence (CDD) includes gaining an understanding of the type of financial activities your customer will be conducting and assessing the associated risk. Ongoing monitoring also is required to ensure your customer stays within the range of expectations and appropriate risk levels for your organization.

Part of the challenge in detecting synthetic identities is that fraudsters can be adept at forging identity documents and creating public records using false/synthetic identities. Tools and solutions also can be evaded, as they are only as good as the data that trains them to detect fraud.

Synthetic identity fraudsters employ numerous tactics to pass identification requirements and make their fictitious identities appear real, including:

- Fabrication of identity documents, such as driver's licenses, passports and state IDs.



- Enrollment in utilities or municipal services.

- Creation of social media profiles for the contrived identities.

Validating identities beyond verification of a customer's name, date of birth, address and identification number offers an opportunity to help further mitigate the risk of a synthetic, as there is more information available to help make an informed decision about whether a person actually exists.

COMBATTING FRAUD WITH A SUITE OF IDENTITY VALIDATION TOOLS

IDENTITY VALIDATION TOOLS

Document Verification

In today's fraud landscape, fraudsters can create fictitious identity documents that often appear valid. Fraudsters use these identities to commit various types of identity fraud, including synthetic identity fraud.

Document ID verification solutions can help seamlessly verify the validity of identity documentation provided by the potential customer. Information provided in the application can also be used to further validate the identity. For example, organizations can ensure the address on the driver's license matches the application data and public record information. These validation processes can be performed on physical documents, electronic documents or both.

Alternative Data

Information gathered from nontraditional or "alternative data" sources, such as public records, can further validate the legitimacy of identity information provided. By piecing together alternative data in conjunction with required data elements, this more complete picture can help determine the identity's validity. Alternative data that can help verify "proof of life" data elements include:

- Commercial licenses (e.g., a fishing license)
- Social media profiles
- Municipal service records
- Utility information
- City hall records

COMBATTING FRAUD WITH A SUITE OF IDENTITY VALIDATION TOOLS

eCBSV

In June 2020, the Social Security Administration (SSA) launched an electronic version of its consent-based verification service (eCBSV), which allows permitted entities to verify if the combination of an individual's Social Security number (SSN), name and date of birth matches Social Security records. Previously, the SSA required the written consent of the applicant via a physically signed document (also known as a wet signature) to disclose the SSN verification information. This was a manual process that could take days or even weeks to complete. Under the new electronic version of this service, applicants can submit their consent electronically in real time. This enables institutions to validate customer information more quickly than in the previous manual process, thereby helping reduce customer friction. The eCBSV service offers another verification tool for financial institutions to use when vetting a potential relationship.

Beginning in February 2022, the eCBSV service was expanded to include all permitted entities wishing to use the service, with enrollment open indefinitely. ***For more information, click here***.

Digital Information and User Activity

A vast amount of information is available online about individuals and their activities. This information can be leveraged to help identify red flags that could indicate a synthetic identity, both during an account opening and when reviewing an existing portfolio. For example, an organization could leverage online information about the user, looking at data elements such as verification of phone number ownership or name associated with phone number to determine if the name matches that of the account applicant. Any mismatch in information could warrant additional investigation. Similarly, it is important to examine information related to actual user activity, such as the geolocation and IP address used to submit an account application, to determine how those data elements compare to the physical address in the application. The more data elements that can be evaluated or compared, the higher the likelihood that an organization can identify the synthetic.

COMBATTING FRAUD WITH A SUITE OF IDENTITY VALIDATION TOOLS

Technology Solutions

Various technology solutions can help validate identities. These generally use multiple data points and analyses to determine risk and identify potential synthetic identities. Analyzing data attributes (e.g., location, device, phone, email, activities) within seconds provides a much more detailed representation of identity than simple ID verification. In addition, technology solutions often have access to a comprehensive data set aggregating information from multiple organizations, offering opportunities for a more in-depth analysis.

CONCLUSION

Given the sophistication of fraudsters, it is paramount that organizations consider validating identities using multiple methods of identity validation to "prove" an identity exists, which can be more effective than relying on any one factor or method of validation.

The synthetic identity fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about synthetic identity fraud and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.