VALIDATING IDENTITIES THROUGH ALTERNATIVE DATA

While it is important to verify an identity using primary elements such as name, Social Security number and birthdate, using additional public or internet-based information or "alternative data" for identity validation can help financial institutions gain a higher level of confidence that the applicant is a real person. The first step in a multi-layered fraud mitigation approach is identity proofing: the process of triangulating data about an identity to help confirm a person is real and who they claim to be.

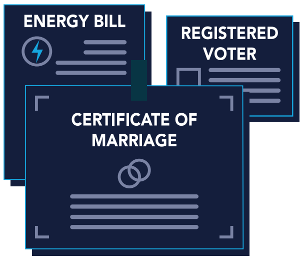
A strong identity-proofing process performed before an account is opened is crucial, as this offers a chance to stop the synthetic identity from becoming a customer. Ideally, identity proofing reviews all available information about the identity – credit history, biometrics, social media presence and so on – to determine if those elements make sense for the identity. Given widespread data compromises and availability of personally identifiable information (PII), it is vital to pull in as many data elements as possible to help validate the identity.

What additional information should be reviewed to determine if an applicant is really a synthetic identity?

CREDIT PROFILE

Data collected at account opening includes the applicant's name, mailing address, phone number, email address, birthdate and Social Security number. Based on the credit profile, does the length of the credit history make sense compared to the applicant's birthdate? Review the tradelines in the credit history to assess the risk level based on the available credit activity. Look for names of co-signers or authorized users that might assist in validating the identity, such as whether a clear connection exists to a relative or company/employer. It's important to keep in mind that the credit report for a synthetic identity may look like a report for a person who has never applied for credit, perhaps prompting a closer look at other identity elements.

VALIDATING IDENTITIES THROUGH ALTERNATIVE DATA



PUBLIC RECORDS

Compare the application information to third-party data. Does the mailing address show other residents at the same address? Is the address an office building rather than a residence, or does no building exist at that address? The applicant's name and address may match public records available online, such as:

- Landline phone number
- Utility information
- Municipal service records
- Property deed and property tax records
- Voter registration and voting records
- Criminal, arrest and court records
- Birth certificates
- Death certificates
- Marriage and divorce records
- Commercial licenses

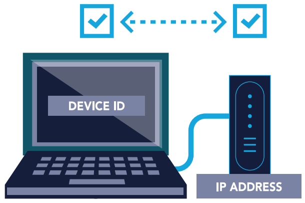
Some records, such as birth and death certificates, may be restricted depending on state laws, although the information could be available through other public records.

ONLINE PROFILE

A social media presence and a history of online activity may help validate that a person is real. The social media presence should be consistent with the applicant's age and address. For example, an applicant's resume posted online should contain the applicant's city, state and a work history that fits his or her expected experience level based on age. Or a social media profile might show relevant posts over time and link to family members and friends. A nonexistent online profile could indicate a higher risk level – but remember that a social media profile could have been created by fraudsters to support a synthetic identity.

Data from an applicant's digital footprint, such as cell phone number or email address, may be found online for comparison to the application. There may be a record of when the email account was created to determine how long it has been active.

If an electronic device was used to submit the application, then its IP geolocation can be compared to the applicant's mailing address for a potential geographic match. To address high-risk applications with inconsistencies or no data, financial institutions could request that the applicant provide additional proof of identity.



INTERNAL DATA REVIEW

A financial institution also can compare application data to existing accounts and other applications across the enterprise. If any of the application data matches, an existing relationship could help authenticate the applicant. Alternatively, a match could mean that fraudsters submitted multiple applications using the same synthetic identity data and created different data combinations to increase their chances for approval of some applications. Also, institutions can review the device and IP address used to submit the application if that information is collected. If multiple applications were submitted from the same computer or IP address, this raises the risk level for those applications and therefore, may require further reviews. Behavioral analytics may indicate potential risks (e.g., slow typing by an applicant who may be unfamiliar with the PII data being entered).

CONCLUSION

Identity proofing can help financial institutions protect themselves from reputational risk and fraud losses due to synthetic identities. No single data element will definitively identify a synthetic identity. Alternative data for a legitimate applicant may be limited – for example, if the applicant did not have access to the internet or did not register to vote. Access to public records varies and financial organizations may opt to use a third-party service to consolidate available data. Organizations can identify discrepancies by comparing data internally (e.g., with other accounts) and externally (e.g., using public records). These discrepancies may prompt further review based on increased application risk levels. Risk indicators may cause financial institutions to request more information from the applicant in the form of government identification and supporting documentation, such as utility bills. To avoid negative impacts and potential financial loss, organizations can leverage alternative data to increase their confidence that an applicant is real and not likely to be a synthetic identity. Conducting periodic validations after an account has been opened can strengthen the opportunity to detect a synthetic identity. These validations often include a review of all customer data available about an identity.

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.