LINK ANALYSIS OVERVIEW

Link analysis is used to identify relationships and connections among data attributes. These connections can flag a potential synthetic identity.

Link analysis can help detect synthetic identities, as fraudsters often reuse personally identifiable information (PII) to create multiple synthetics. Implementing "fuzzy logic" – a degree of truth – can identify close matches, as fraudsters may make minor alterations to real PII. By identifying close matches rather than "perfect" matches, link analysis can help identify multiple synthetics, and perhaps even multinational crime ring activities.

At account opening, link analysis can be deployed to determine if an application's data elements have been reused by another identity. For example, a Social Security number submitted under the name John Smith might already exist within your portfolio with the name of Josh Jones. Identifying these types of similarities prior to account opening can help you assess the risk, investigate further and take appropriate action.

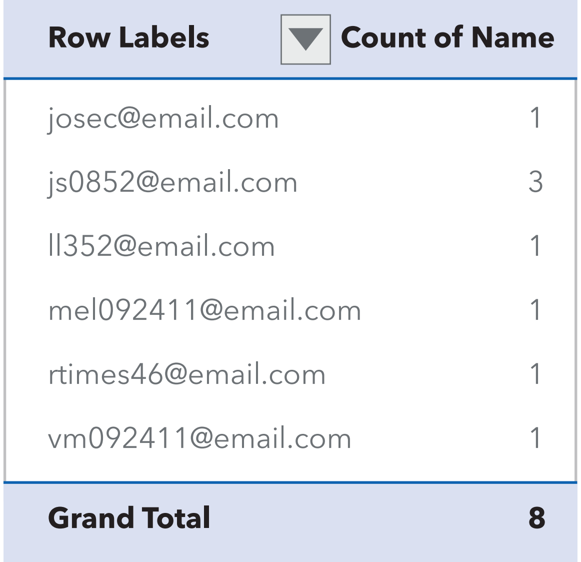
Similarly, after a relationship has been established, link analysis can help identify commonalities that are potential red flags. For instance, you might see a common phone number and IP address across multiple relationships. This could raise a red flag, as it is less likely for the same phone to be used to access multiple relationships, particularly among people who are not apparently related.

Some potential data elements for link analysis include:

- Applicant name, mailing address, phone number, e-mail address, birthdate and Social Security number.
- Authorized users from credit history (if any were included).
- Device ID and IP address used to access the account.
- Previously identified synthetic identity fraud data.
- Account activity, such as payments to an account or incoming credits from an account.

LINK ANALYSIS OVERVIEW

Link analysis can be a powerful tool in the fight against synthetic identity fraud. The more data points you can pull into your analysis, the greater potential to find commonalities. While various technology resources can help with your link analysis, something as simple as a spreadsheet can be utilized if a more complex vendor solution is not available. By starting small with one data point as your anchor, you can evaluate subsequent data sets to determine if there is a potential linkage between the anchor and the rest of the data. A simple pivot table also can be used to determine possible linkages and irregularities, such as the same email address associated with more than one name within your portfolio.



Row Labels ▼	Count of Name
josec@email.com	1
js0852@email.com	3
ll352@email.com	1
mel092411@email.com	1
rtimes46@email.com	1
vm092411@email.com	1
Grand Total	**8**

In addition, more sophisticated tools can help you more quickly analyze large data sets to identify potentially suspicious relationships, such as "one to many" or "many to one," meaning one data attribute associated with multiple relationships or vice versa. It is much less common for legitimate customers to share a device, email address and phone number across hundreds of relationships. However, this pattern is not uncommon with synthetic identities, as they are all controlled by the same fraudster. Patterns such as the one just described are evident when using a link analysis tool.

LINK ANALYSIS OVERVIEW

555-4456
555-8340
555-5643
555-5643
555-4506
555-0021
555-5643
555-5643
555-5643
555-6098
555-1864
555-8899
555-1181
555-0496
555-3245
555-5643
555-7956

Because synthetic identity fraud may appear to be normal consumer activity, looking for data attribute commonalities across products and relationships is an important part of synthetic identity fraud detection. Data elements from an application that match an existing account or another application can indicate potential fraud. This approach relies on access to data for comparison but does not require advanced technical solutions or software to be successful. By deploying link analysis, you can potentially identify these commonalities and take appropriate actions to protect your institution.

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.