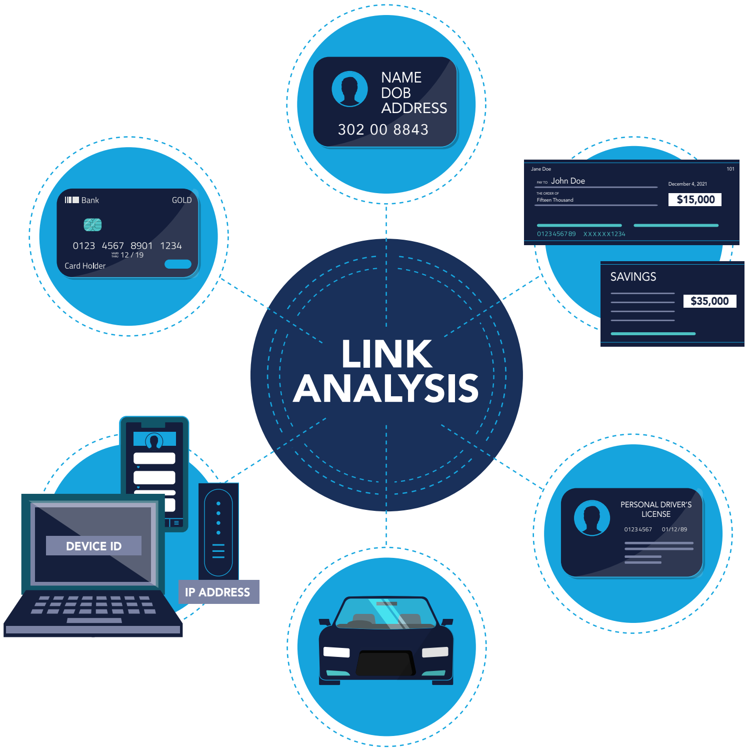
USE CASE: CREDIT UNION ORGANIZATION LINK ANALYSIS

Fraudsters continue to advance their fraud tactics and technological capabilities. As a result, financial institutions may want to continually update their fraud mitigation using new technologies and incorporate customer data from multiple access points. Customer information can be ascertained from various banking instruments and across channel types to identify relationships and common characteristics of known "bad actor" information. This link analysis allows financial institutions to use shared intelligence from multiple data points for a 360-degree view of a customer. Examples of link analysis to help detect synthetic identities include:

- Identifying banking customers using the same Social Security number, but different identity information (such as name and date of birth).
- Identifying potential fraud networks via review of a high volume of applications with differing customer information that were all submitted through the same IP address or device ID.
- Identifying commonalities amongst applicant information – such as a high number of customer accounts linked to the same mailing address.
- Linking identities that are authorized users on the same high volume of tradelines.



Service providers can perform link analysis and share information with multiple financial institution clients. For example, a credit union service organization developed an in-house link analysis program, allowing it to connect transactions and customer data across various platforms, channels, banking instruments and customers to help identify potential fraud. Data scientists then used the linkages and commonalities to research anomalies in the customer data. This credit union service organization estimates its link analysis program has prevented millions of dollars in fraud losses.

USE CASE: CREDIT UNION ORGANIZATION LINK ANALYSIS

The organization's successful uses of link analysis include:

- **Identifying Customer Anomalies**
  Link analysis detected activity that was inconsistent with a member's typical transaction pattern. The fraud intelligence solution blocked the attempted fraudulent card transactions that would have been approved if not identified as transaction anomalies.

- **Blocking Attempted Account Takeover**
  The credit union service organization monitored transaction activities across multiple platforms and correlated failed authentication of a user account on multiple platforms. Fraud intelligence then flagged these accounts before losses occurred at the credit union organization.

Link analysis programs demonstrate the effectiveness of identifying and sharing known synthetic and bad actor information among organizations.

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.