Synthetic Identity Fraud

The hidden threat costing you revenue

The problem with synthetic identities

Synthetic identity fraud is one of the fastest-growing threats today. Most businesses are likely struggling with this threat and don't even know it — letting money go to waste and exposing the company to fraud risk.

Synthetic identity fraud occurs when a fraudster blends a combination of real or fictitious identity components to create a new identity. Typically, fraudsters create these identities and nurture them for months to years — opening credit cards and paying them off — so that they look legitimate to lenders and credit reporting agencies. Once an acceptable credit history has been established, the fraudster maxes out the charges, leaving the lender with significant financial losses.

These manufactured identities are used for short term gain and then abandoned. When this is the case, there is no one for the lender to contact in order to collect funds. This poses a problem for organizations as misclassified non-payment matters get sent to collections, further wasting resources.

How fraudsters establish credit

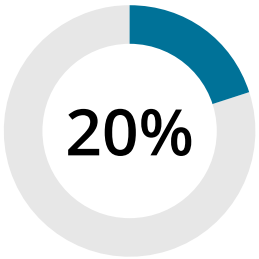
There are two ways for the fraudster to establish credit.

New Account Fraud

Fraudsters create a new identity using a mix of real and fake information, then build credit slowly by making small purchases and paying overtime to establish a positive credit history.

Authorized User Abuse

Fraudsters create a synthetic identity and add the identity as an authorized user on an existing, legitimate credit card account.



Synthetic identity fraud is the fastest growing fraud classification in the US and now accounts for **20% of credit losses** in the U.S. Financial system[1].

How to stop synthetic identity fraud

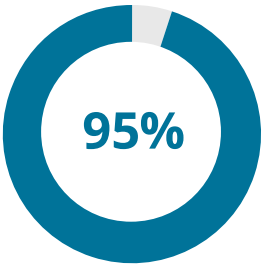
Equifax offers a multi-layered approach to protecting your business from synthetic identity fraud.

Synthetic Identity Alerts

Synthetic Identity Alerts can be used during account origination to sort applications that trigger an alert into a manual review process. For example, financial institutions can use them for credit card, demand deposit, personal loan, and auto loan account opening. Delivered in batch or real time, these alerts use patent-pending machine-learning algorithms to detect synthetic ID behaviors and patterns at various entry points.

Account and Portfolio Management

Synthetic Identity Alerts can be used to append existing portfolios to pinpoint accounts that may have been opened using synthetic identities. Once identified, you can use existing strategies for further verification and authentication.



95% of synthetic identities are not detected during the onboarding process[2].

Key benefits of Synthetic ID Alerts

Actionable Insights

Leverage more actionable insights while maintaining low false positive rates.

Real-Time Responses

Cloud technology enables Equifax to facilitate real-time responses to suspicious user activity.

Matching Logic

Enable classification of authorized user abuse and consumers potentially committing synthetic identity fraud.

Machine Learning (ML)

ML algorithms help discover unique behavior patterns associated with identity aspects.

Synthetic identity losses by segment[3]:

$8.0B
Auto

$2.5B
Unsecured credit products

$2.0B
Bank cards

$1.0B
Telecommunications

Conclusion

Successfully protecting your business against fraud requires a multi-layered approach. Synthetic Identity Alerts are part of an integrated suite of identity verification, authentication, and fraud detection solutions. Our proprietary and differentiated data helps assess modeling behavior, rather than just data checking — which can provide a better output for prevention.

Contact your sales rep to learn more about our identity solutions.

1 Javelin Strategy & Research. (2024). 2024 Identity Fraud Study: Resolving the Shattered Identity Crisis. Javelin Strategy & Research.
2 Themis. (2025). 2025 Fraud Trends. Themis.
3 Federal Trade Commission. "Fraud and ID Theft Maps." Tableau Public. Accessed April 7, 2025.