



Case Study

Tackling fraud initiated through authorized user abuse

Credit Issuer customer

CHALLENGE

Minimize losses due to synthetic identity accounts

SOLUTION

FraudIQ® Synthetic ID Alerts enabled credit issuer to efficiently identify card accounts likely to be a result of authorized user abuse

RESULT

Identified more than 100,000 synthetic identity accounts during account origination resulting in more than \$25 million in potential charge-offs in one year

Challenge

A leading credit card issuer was struggling with rising unrecoverable charges. The customer knew that a portion of card accounts were a result of synthetic identities created via authorized user abuse, but did not have an efficient way to identify them.

Solution

With FraudIQ Synthetic ID Alerts, the credit issuer was able to:

- **PINPOINT** card accounts that were likely opened using synthetic identities, in which fraudsters had piggybacked good consumers' credit
- **PROTECT** against fraud write-off charges resulting from lack of payment on card balance or interest charges from synthetic identity accounts
- **LEVERAGE** Equifax AI-driven machine-learning algorithms using multiple data sources to detect synthetic identity behavior and patterns

Results

A portfolio analysis which appended FraudIQ Synthetic ID Alerts to the credit issuers' card portfolio revealed:



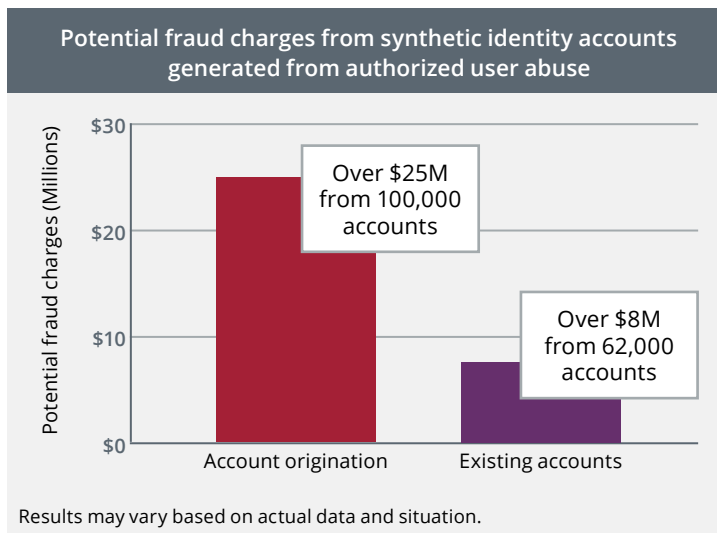
More than **100,000** synthetic identity accounts identified during **account origination** could result in more than **\$25 million** in potential charge-offs in just one year



More than **62,000** synthetic identity accounts in its **existing portfolio** could result in more than **\$8 million** in potential losses in just one year



After seeing the results of the analysis, the credit issuer instituted a **one-time scrub** of its card portfolio as well as **ongoing monitoring** during account origination, helping to **protect against millions** in fraud write-off charges



Authorized user abuse defined: Sometimes called credit boosting or piggybacking, Authorized User Abuse occurs when low-risk primary card owners "rent" their tradelines with extensive credit histories, high credit limits and solid repayment profiles to fraudsters.

Product Spotlight

FraudIQ Synthetic ID Alerts

protect businesses from financial losses by identifying risks associated with synthetic identity fraud and potential malicious intent, and mitigating false positives.

Using machine-learning algorithms, **FraudIQ Synthetic ID Alerts** detect anomalies around consumer identity and synthetic identity behaviors and patterns that are industry-specific for identity fraud detection and prevention.

Find out how Equifax can help your business identify authorized user abuse to mitigate fraud at equifax.com/business/prevent-fraud