USE CASE: CAR LOANS

INTRODUCTION

Synthetic identity fraud impacts financial institutions of all sizes and across multiple credit products and accounts. Criminals often cultivate multiple synthetic identities at the same time to build positive credit histories until they see an opportunity to maximize the amount they can steal. Recent headlines about prosecuted cases involving synthetic identities show their widespread occurrence and financial impact. Financial institutions can share their learnings to promote awareness and illustrate these fraud threats.

OVERVIEW

A large credit union with security and fraud prevention tools was targeted by a synthetic identity fraud ring. Fraudsters exploited a product and process gap using synthetic identities even though the credit union was using several fraud detection tools, consistent with industry standards, and investing in security upgrades. A criminal ring used synthetic identities with well-established credit to submit multiple applications for loans to purchase used vehicles. The credit union lost $420,000 when the loans were not repaid.

SCENARIO

Synthetic identities were created over several years to establish positive credit histories and solid credit ratings. Loan applications were submitted by what appeared to be "average" consumers to fund the purchase of used cars. Based on their good credit scores, these synthetic identities were not required to show proof of income to obtain loans. The loans were approved based on the financial institution's credit decisions and the process did not include a step to check for synthetic identities or leverage fraud intelligence about the applicants.

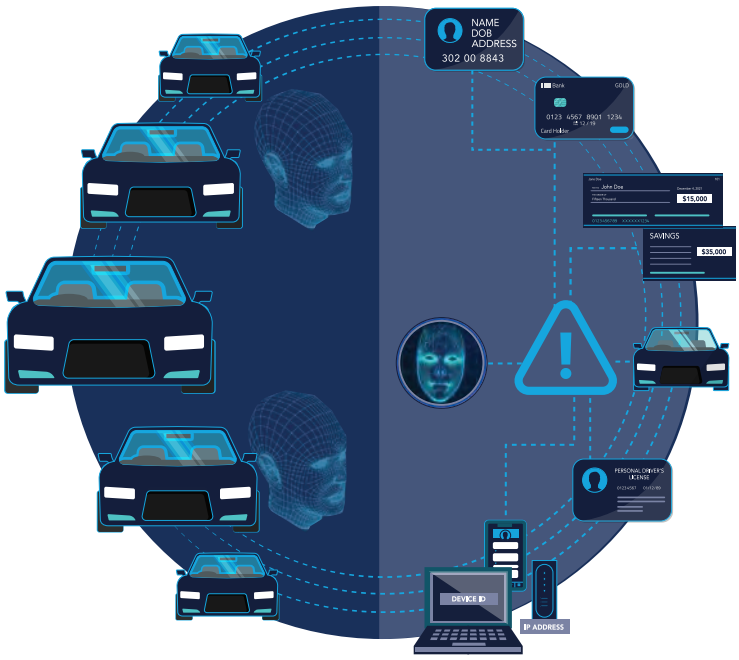
RESPONSE

The credit union assessed its loan approval process, available anti-fraud tools, the fraud loss amount and the potential for future losses. Two key findings:

- The loan approval process lacked the necessary fraud review to look for synthetic identities or recognize red flags for applicants.
- The existing fraud detection tools were rules-based, which required each new fraud scenario to be identified before rules could be defined, deployed and fine-tuned without creating unnecessary friction in the approval process.

USE CASE: CAR LOANS

The credit union's executives and technology leaders pursued a solution that would proactively detect new fraud threats by using machine learning rather than static rules. The platform is designed to adapt to new threats and provide fraud intelligence with new information. The solution included the ability to process a large volume of data and incorporate human insight and expertise into the analysis. In product testing, it was estimated that the new solution would have detected about 75% of the fraud ring activity. Once deployed, the new anti-fraud platform reportedly detected and prevented more than $1.8 million in fraudulent activity across products and scenarios. This institution also is working to expand its machine learning fraud detection capabilities to other functions, such as customer onboarding.



The credit union shared its learnings from this scenario with other credit unions to raise industry awareness about synthetic identity fraud.

The credit union also is using a service to promote further information sharing with other financial organizations, using "double-blind" encryption that allows it to share suspected synthetic identity fraud profiles without disclosing any personally identifiable information (PII).

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.