Digital Fraud Wiki

FRAUD DEFENSES

Crowdsourced Abuse Reporting
Device Fingerprinting
Email Reputation Service
IP Reputation Service
SR 11-7 Compliance
Supervised Machine Learning
Two-Factor Authentication (2FA)
Unsupervised Machine Learning

FRAUD TACTICS

Bot Attacks
Call Center Scams
Device Emulators
GPS Spoofing
P2P VPN Networks
Phishing Attacks
SIM Swap Fraud
URL Shortener Spam
Web Scraping

FRAUD TYPES

App Install Fraud
Application Fraud
Bust-Out Fraud

Loan Stacking

What is Loan Stacking?

Loan stacking refers to the practice of getting approval for multiple loans or lines of credit simultaneously within a short period. Loan stacking generally happens online and can be done by either individuals or businesses. It is not illegal to “stack” loans, but financial institutions lose billions of dollars every year to the process because many loan stackers commit application fraud – intentionally default on the loans they take out.

There are three types of loan stacking: credit shopping, credit stacking, and fraud stacking. The first two, while problematic for financial institutions, are nonetheless legal. Credit shopping is where borrowers apply for multiple loans to get the best interest rate. Credit stacking is where legitimate buyers apply for credit without realistically having the means to repay. The third type is fraud stacking, in which fraudsters apply for multiple loans with no intention of paying them back.

What Should Financial Institutions Know About Loan Stacking?

The growing availability of instant credit approval from financial institutions has allowed consumers and fraudsters alike numerous opportunities for loan stacking. Financial institutions are losing billions of dollars every year because of loan stacking by fraudsters

Loan Stacking
Synthetic Identity Theft

and legitimate borrowers. Large, organized crime rings often orchestrate loan stacking schemes that aim for huge payouts from banks.

Fraudsters use sophisticated, involved strategies like identity theft and bust-out fraud to achieve maximum profit from loan stacking. For example, a fraud ring might create identities using stolen social security numbers and personal information obtained from phishing schemes. The fraud ring would apply for hundreds of loans distributed among multiple banks using the stolen identities. Once the loans are approved, the fraudsters gradually incubate each account- emulate legitimate user behavior, make the payments on time, and then suddenly "bust out" maxing out all of the accounts. The fraudsters disappear, and the lenders incur significant losses due to the defaults.

- Five individuals were recently arrested for allegedly attempting to steal more than one million dollars from five major credit unions. The fraud ring spent a year gradually filing more than one hundred loan requests electronically using stolen names and social security numbers. The fraud ring managed to steal more than $200,000 with this fraud stacking scheme.

Financial institutions need a solution that detects fraudulent loan and credit card applications before they reach the collections stage.

DataVisor Detects Loan Stacking

Application-level detection is critical for achieving genuinely proactive fraud management. Whereas most legacy systems still in use today operate solely at the transaction level—and are inherently reactive by nature—advanced, AI-powered solutions such as DataVisor's dCube incorporate application-level analysis as well. This enables systems to flag suspicious activity before attacks launch and damage is caused. In the case of loan stacking, a reactive, transaction-level approach cannot identify fraud or instigate action until after malicious activity takes place. dCube, on the other hand, can correlate patterns and surface cross-account links that indicate coordinated application activity while an attack is still being planned, or early enough in the process that no damage is caused. This is particularly important for instances such as the attempted credit union theft, in which fraudulent accounts incubated for extensive periods of time before being put to use. Coordinated management of incubating malicious accounts can only be detected by solutions such as dCube; solutions that make holistic analysis and contextual detection possible, and which leverage the power of unsupervised machine learning to flag suspicious accounts early enough to prevent downstream damage.

Additional References

Solution: Financial Services

Solution: Application Fraud

Source: How fraudsters are gaming online lenders, American Banker

Source: Massive loan fraud ring busted: Hundreds of victims targeted, ABC, Inc., WLS-TV Chicago

Source: $8B In Bad Credit Card Debt Write-Offs Worry US Banks, PYMNTS.com

Source: Big Four U.S. Banks Hit With $12.5B In Credit Card Losses, PYMNTS.com