Fresh Schemes to Perpetuate Synthetic Identity Fraud

technology fraud protection

Summary: Would-be thieves are coming up with more ways to attempt synthetic identity fraud. We delve into some of the schemes you should be on the lookout for, and detail some methods to detect, validate, and minimize losses from such fraud.

As synthetic identity fraud involves the use of at least one authentic piece of personally identifiable information mixed in with fake identifiers, no movie depicts this more innovatively than the 1997 film, “Face/Off” — in which face transplants take impersonation to a new level.

In the film, FBI Special Agent Sean Archer (played by John Travolta) undergoes facial transplant surgery to pose as comatose Castor Troy (played by Nicolas Cage) to infiltrate his operation. Troy wakes up from his coma, however, and contacts his gang to force the doctor to put Archer’s face on him, thus completely swapping identities with each other.

In real life, fraudsters are also coming up with novel ways to perpetuate synthetic identity fraud, which means using some legitimate information that was stolen. This could mean using the name, social security number, and birthdate of a real person, and then fabricating additional information such as a mailing or billing address, phone number, email address, or digital footprint.

Here are some fresh fraud trends that you should be on the lookout for:

New ways to obtain children’s identities. Child synthetic identity fraud has been around for decades, but fraudsters are now obtaining that information from both the dark web and social engineering tactics — either through the social media accounts of children themselves or those of their parents. They may also dupe employees of school districts to volunteer sensitive information.

Automated auto loans. The digitalization of auto loan applications, originations, and funding has enabled fraudsters to use synthetic identities to obtain financing en masse for numerous luxury vehicles, after which they sell them for substantial cash. Automated loan processes also enable people with shoddy credit histories to substitute fake creditworthy information to get a loan at a better rate, or even a loan at all.

Buy now, pay later (BNPL). Fraudsters are impersonating consumers with poor, limited, or nonexistent credit histories to purchase goods via BNPL and then skip out on the payment installments.

How to Detect Synthetic Fraud

Luckily, there are some tactics that you can employ to minimize losses from attempted synthetic identity fraud:

Detecting red flags within a customer’s application or account. Further identity validation may be necessary if the following are present:

- A large amount of unsecured debt.

- A high number of recent credit inquiries.
- A mismatch between the accountholder’s age and the duration of credit history.
- An inflation of credit file depth.
- A suspicious mailing address.
- Recently issued contact information.

Spotting duplicates. Some fraudsters might use the same stolen info across multiple fraudulent applications, making slight changes to each one. This can include any of the following signs:

- Similar or matching contact information.
- Matching Social Security numbers.
- Identical digital footprint.

Validating identities. Since fraudsters typically fabricate driver’s licenses, create fictitious social media profiles, and even enroll for utility services at fictitious addresses, you should leverage alternative data to verify identities. Some tools you can use are credit profiles, public records, and other kinds of online profiles. Your team should also employ “identity proofing” — triangulating identity data across the application, documents, social media, and additional online presence of the applicant to determine if all the data makes sense for the “identity” applying for the product or service.

Leveraging technology. The Federal Reserve recommends that institutions employ technology solutions, particularly those with AI-powered and machine-learning capabilities, to prevent and mitigate synthetic identity fraud. Machine learning can also detect patterns of “bad data” across systems, including insights about new fraud cases gleaned from law enforcement and other outside sources.

More robust solutions can now be integrated into an institution’s existing fraud detection processes to do the following:

- Perform sophisticated identity proofing to detect applications made by synthetic identities.
- Provide early account monitoring to detect and defend against fraudulent accounts from the start.
- Conduct ongoing monitoring once accounts have matured, as fraudsters often wait until institutions have let their guard down.

Acquaint yourself with the newest forms of synthetic identity fraud to stay on top of would-be thieves. Arm your institution with increased know-how — as well as robust technology solutions to stop attempted fraud in its tracks and minimize the impact on your institution and identity fraud victims.

START SMALL AND UPGRADE LATER WITH CECL FIT

ECONOMY & RATES

Rates As Of: 04/21/2023 06:59AM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	5.12	0.27	0.70
6M	5.06	0.12	0.30
1Y	4.74	0.14	0.04

2Y	4.16	0.13	-0.27
5Y	3.66	0.08	-0.35
10Y	3.56	0.09	-0.31
30Y	3.77	0.12	-0.20

FF Market	FF Disc	IORB
4.83	5.00	4.90
SOFR	**Prime**	**OBFR**
4.80	8.00	4.82