BANC OF CALIFORNIA | TOGETHER WE WIN™

SYNTHETIC IDENTITY FRAUD

Criminals create fake identities and use them for credit scams.

Synthetic identity fraud typically targets financial, insurance, healthcare and government payment systems.

When we think about payment fraud, we usually think of it as hijacking the identities of real payees (people, businesses or other organizations) and using them to trick payors into making payments to accounts that appear to be entities they know.

But, the fastest-growing form of financial fraud in the U.S. is synthetic identity fraud based on fictitious Personally Identifiable Information (PII) such as a Social Security number, a modified version of existing PII or a combination of the two.

This type of fraud is most pervasive as a threat to credit card companies and banks, but criminals also target insurance companies, government agencies, and businesses that extend credit.

The scam revolves around building credit over time.

It begins with a new identity that has no credit history. A synthetic identity fraud scheme takes time to develop. Scammers often start on the dark web, purchasing little-used PII and other information (such as that of children or seniors) that has been compromised by data breaches, social engineering or other methods. Other times, they concoct it from scratch. Fraudsters impersonate HR departments, directing employees to sign in using what appear to be official links.

Then they apply for credit, knowing that they will be rejected. But by applying, they trigger the creation of credit profiles. Then they repeatedly apply for credit from companies that offer cards to higher-risk applicants. Once they obtain limited credit, they make small purchases and pay for them in order to build credit histories over time.

Scammers accelerate their credit through "piggybacking."

Often, scammers build credit by attaching themselves as authorized users to existing credit cardholders using the compromised data they've acquired. The scammers do not have cards assigned to them and no activity is reported, but they are using their unwitting hosts' good credit to burnish their own.

Inevitably, the fraudster maxes out and disappears.

With a positive credit profile built, a fraudster will "bust out" by maxing out the credit line and disappearing. In some cases, they'll milk it for even more by claiming, ironically, that they've had their identities stolen, to effectively double their take when the charges are removed. Also, they may enhance their take by maxing out their credit and paying it off with a phony check.

What can you do to fight synthetic identity fraud?

This type of fraud is difficult to detect, but there are precautions you can take to spot it and actions to take if you suspect it.

- Be careful about what you post on social media
- Check your credit regularly for suspicious activity such as new authorized users or connections with organizations you don't belong to
- Use multilayered controls and tools to spot red flags before setting up accounts or approving loans
- Report suspicious activity to the Nationwide SAR (Suspicious Activity Report) Initiative and NSI, a joint effort of the DHS, FBI and other law enforcement partners. For information, visit https://www.dhs.gov/nsi

What kinds of information can fraudsters buy on the dark web?

- Credit/debit card and information from PayPal® and other services
- Social Security numbers
- Driver licenses and passports
- Medical records
- Diplomas
- Subscription and loyalty program information

2020 AFP® Payments Fraud and Control Survey | www.AFPonline.org

EQUAL HOUSING LENDER FDIC