SYNTHETIC IDENTITY FRAUD: WHAT IS IT AND WHY YOU SHOULD CARE?

WHAT IS SYNTHETIC IDENTITY FRAUD?

Synthetic identity fraud is defined as the use of a combination of personally identifiable information (PII) to fabricate a person or entity in order to commit a dishonest act for personal or financial gain.

Synthetic identity fraud consists of two main components:

1. The creation of a synthetic identity
2. Using that identity to commit fraud

Conventional identity theft occurs when one's existing identity is stolen. In contrast, synthetic identity fraud occurs when a new identity - a synthetic identity - is created. There are various approaches to creating a synthetic identity, but all include piecing together PII, such as a name, date of birth and Social Security number (or other government-issued identifier) to establish a new person or entity.

WHY IS IT IMPORTANT TO KNOW ABOUT SYNTHETIC IDENTITY FRAUD?

- **S**ynthetic identity fraud accounts for substantial financial loss.
- Synthetic identity fraud is growing in frequency and impact.
- Synthetic identity fraud is often undetected by traditional fraud models.
- Synthetic identity fraud is extremely pervasive, with numerous avenues for application.
- Synthetic identity fraud can have a devastating impact on individuals.

The use of synthetic identities can negatively affect individuals. When a synthetic identity was created using an existing Social Security number (SSN), the individual who legally owns that SSN is likely to have poor credit ratings and/or outstanding debt as a result of fraudulent activity associated with that SSN (albeit under a separate identity).

Some of the more vulnerable populations, such as children and the elderly, are key targets of fraudsters wishing to create synthetic identities. These populations are attractive to fraudsters as they aren't typically active credit users and, therefore, are not as likely to notice fraudulent activity.

CHILDREN ARE COMMON VICTIMS OF SYNTHETIC IDENTITY FRAUD

Why:

- Parents usually don't actively monitor their children's identities, credit scores, etc.
- Children do not typically use SSNs until they are old enough to drive, be employed or apply for individual credit lines.

Impact:

- Negative or derogatory information associated with the SSN may not be discovered until the child reaches the upper teens, resulting in several years of fraudulent activity tied to the SSN that must be remedied.
- This can affect the individual's employment opportunities and/or creditworthiness.

HOW TO PROTECT YOUR PERSONAL INFORMATION

- Create strong passwords; use different passwords for each account; create unique security questions/answers
- Be diligent in communications: if it seems suspect, trust your instincts; don't click on links from unknown senders; don't provide or confirm personal information when contacted by another party
- Physically protect your personal information: lock up sensitive information; securely destroy unneeded documents
- Monitor and protect your credit: request your credit report and review it; safeguard your accounts