What You Need to Know About Synthetic Identity Fraud

How Fraudsters Create Synthetic Identities

1. Fabrication
   - Creates a fake Social Security number, steals one, or purchases a stolen one.

2. Legitimization
   - Adds other info to create a fake identity (often times as an authorized user) and uses it to apply for credit.

3. Monetization
   - Creates a fake Social Security number, steals one, or purchases a stolen one.
   - Legitimization: Adds other info to create a fake identity (often times as an authorized user) and uses it to apply for credit.
   - Action: Uses the synthetic identity to apply for credit.

4 Keys to Fighting Synthetic Identity Fraud

1. Use the vast resources of credit reporting agencies and data aggregators specializing in fraud.
2. Combine multiple techniques and layered approaches for fraud detection.
3. Use machine-learning algorithms to help identify discrepancies in a fashion that is not easy to detect.
4. Use data analytics to detect linkages and suspicious patterns indicative of phony or manipulated identities.

Tell-Tale Signs of Synthetic Identity Fraud

- Few “real-life” indicators, such as relatives, social media accounts, vehicle registrations, etc.
- Rapid increase in account applications
- Hyper-monitoring of credit score
- High rate of approval of multiple accounts

Learn more about synthetic identity fraud and how Equifax can help.