NICE Actimize

Insights Article

Synthetic Identity Theft—What Is It and How You Can Prevent the Risk

Introduction

Financial crime is becoming increasingly sophisticated and frequent, evolving alongside the digital economy and the implications of the data-first era. Synthetic identity theft, one of the fastest accelerating forms of financial crime in the U.S., is a particularly complex security threat contributing to the growing risk landscape and reshaping technological investment priorities for financial services organizations (FSOs).

What is Synthetic Identity Theft?

Synthetic identity theft is a type of account fraud—a criminal combines real and fake information (names, social security numbers, addresses, dates of birth, etc.) to create a new identity. The real information details are usually stolen.

Synthetic identity theft stems from criminals falsifying identities to steal money via new credit lines or accounts. In the case of synthetic identity theft, only part of the identity is legitimate, or even none of it. Identities are often cultivated for extended lengths of time and are infrequently detected and reported because there's no specific consumer victim to communicate suspicious account activity.

Due to occasionally ambiguous industry definitions, synthetic identity theft is sometimes lumped together with first-party or third-party fraud. To clarify, first party fraud occurs when an individual is purposely misrepresenting their information to commit fraud. Third-party fraud, sometimes called "true identity fraud," occurs when a fraudster steals and uses another person's Personally Identifiable Information (PII) to obtain a loan, open new accounts or access existing ones.

Generally, there are two primary categories of synthetic fraud:

- **Manipulated:** Minimal alterations are made to an authentic identity, like the address and date of birth (DOB), while retaining the SSN and name. This can then be used to access credit or attached to an existing credit product to fast-track identity building.
- **Manufactured:** Data is patched together from multiple real identities, such as the DOB from one person, the address from another, an SSN from a third, etc., to create a new false identity. Alternatively, the information might be entirely fabricated apart from a valid SSN, or derived from a random sequence of numbers selected from the number range used by the Social Security Administration (SSA) when distributing SSNs.

Drivers of Synthetic Identity Theft

As FSOs amplify digital transformation initiatives and eliminate the need for physical interactions, a climate susceptible to synthetic identity theft has emerged, making it difficult to prove that an identity is authentic. This, and other factors, have opened up a gateway of possibilities for fraudsters.

Valuable PII data proliferates and can be illegally acquired on the dark web, or credit files may closely resemble those of actual people, like young adults, who are beginning to build a credit history.

Fraudsters can elude detection for years when using stolen SSNs from children because children can't apply for credit until they're 18 years old. Young adults who are just creating credit identities for the first time, individuals who are new to the country, divorced women, incarcerated individuals and the elderly are just a few of the demographics vulnerable to exploitation by criminals because they represent identity groups that are challenging to authenticate and difficult for FSOs to decline.

Other enablers of synthetic identity theft include:

- Lack of a single source of truth surrounding identity verification.
- Inaccurate identity data across data sources, leading to more common red flags that are easy to overlook.
- Siloed identity verification data sources.
- Traditional tools that fail to detect fraud and prevent financial losses once a synthetic identity enters an institution and matures.

All these drivers have added an entirely new dimension to the scope of cyber-vandalism, and sparked urgency for new investments in automated fraud prevention and management solutions. FSOs need to incorporate protection across every phase of the application lifecycle, execute early monitoring of new accounts and facilitate continuous monitoring of all associated account data.

How to Prevent Synthetic Identity Theft

Data and intelligent technologies are the most effective weapons in the fight against synthetic fraud. Temporary fixes, like linking photos, videos or selfies to identity verification processes have been shown to reduce fraud but won't be sustainable long-term given the proliferation of deep fakes. The key is to use copious quantities of data to authentic identities and close information gaps and use advanced analytics to recognize and manage risks across the entire application lifecycle.

An AI-powered enterprise fraud management system can connect all the diverse data types and sources, and facilitate the following regarding identity authentication:

- Data corroboration to establish trust and ensure authentic applicants can get through the system. This includes validating phone numbers and emails and establishing real-time possession or accessibility and verifying that devices and personas have been previously connected.
- Evidence of a person's existence in relationship to their specified address and information.
- Verifying that all this information is a likely fit for the applicant's age, occupation, and nationality.

FSOs should strategically support these intelligent capabilities by further investigating anomalies and gaps, such as why a 45-year-old with a steady job and income has never been previously visible, for example. Additionally, velocity should be monitored to prevent multiple applications from being submitted from the same device, email or phone across a short time period.

Together, this provides a modern control framework from which FSOs can better guard their organization against synthetics, reimagine the customer experience and advance transformation initiatives.

Embedded Fraud Management Fuels Innovation

The future of digital fraud is already here, and FSOs need to simultaneously enable rapid digitization while protecting their sensitive, high-value assets against growing, complex threats. As FSOs prepare for the next iteration of digitization and the accompanying risks and opportunities, they need a smart fraud management solution that drives a holistic approach to fraud detection and prevention.

Fast, accurate synthetic fraud detection during time of application or account opening is crucial but concerns of potentially inconveniencing customers can impact broader efforts surrounding robust identity verification checks. IFM-X’s New Account Fraud is a smart end-to-end fraud management solution that can help in this regard, enabling FSOs to orchestrate quick adjustments to new fraud risks and mitigate new account fraud while maintaining a superior customer experience to minimize abandonment rates and boost new account acquisition.

IFM-X’s New Account Fraud answers this need, providing the ability to streamline identity verification processes and use identity risk scores and identity-related intelligence combined with behavioral analytics to detect synthetic identity risks during new account phases. This modernizes account opening journeys and allows FSOs to realize the “True North” of autonomous fraud operations and investigations.

To explore more information about protecting your organization from synthetic identity theft visit the IFM-X New Account Fraud solution from NICE Actimize.

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance.

The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

www.niceactimize.com