NICE
ACTIMIZE

Insights Article

How to Tackle the Pervasive Challenge of Synthetic Identity Fraud

Introduction

Financial crime is becoming increasingly sophisticated and frequent, evolving alongside the digital economy and the implications of the data-first era. Synthetic identity fraud, 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).

> **Cyber-criminals are exploiting gaps in fraud prevention and management capabilities and the unprecedented shift to digital channels to perpetrate financial fraud at scale, like using synthetic identities derived from a mixture of stolen and falsified information to commit new account fraud and application fraud.**

Recent research from Aite Group approximates that by 2023, synthetic identity fraud for unsecured U.S. credit products will total $2.42 billion1 annually, and will account for the majority of debit deposit account (DDA) losses associated with application fraud, which are forecasted to reach almost $1 billion[1] annually.

The financial services industry is particularly vulnerable to fraud schemes due to the nature of the critical data and financial assets under their jurisdiction. More so, FSOs must combat synthetic fraud without causing additional customer friction that could potentially compromise the customer experience.

The historical lack of effective solutions to help detect and combat synthetic identity fraud, coupled with the absence of source data to verify individual identities, makes this growing issue even more challenging for FSOs to efficiently combat. Advanced analytics and artificial intelligence-driven fraud prevention and management solutions are proving to be powerful tools in the ability to proactively anticipate, respond to and mitigate fraud with real-time detection, decisioning and responsiveness.

What is Synthetic Identity Fraud?

Synthetic identity fraud stems from criminals falsifying identities to steal money via new credit lines or accounts.

In the case of synthetic identity fraud, 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 fraud 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, a 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.

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.

Drivers of Synthetic Identity Fraud

As FSOs amplify digital transformation initiatives and eliminate the need for physical interactions, a climate susceptible to synthetic identity fraud 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 fraud 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 of 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.

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.

Proactively Tackling Synthetic Fraud

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 of 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 of this information is a likely fit for the applicant's age, occupation and nationality.

While this can be built as rules, enabling repeatable, reliable, and data-driven outcomes is better facilitated by machine learning (ML) models trained and developed from high quality historical data. This also allows fraud detection and prevention frameworks to be continuously improved and scaled, which is one of the core features of the IFM-X's New Account Fraud solution. A cloud-based model is another important component in synthetic fraud detection and prevention, as it offers the agility and maximized processing necessary to optimize fraud risk model development.

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.

To explore more information about protecting your organization from synthetic identity fraud with the IFM-X New Account Fraud solution from NICE Actimize, click here.

1. Fooshée, T. (n.d.). Application Fraud: Accelerating Attacks and Compelling Investment Opportunities (2020 ed., Vol. November, Rep.). Aite Group.

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