Tip sheet

Keeping synthetic identities out

Synthetic identity (SID) fraud isn't a victimless crime. When a synthetic ID enters your portfolio, no single individual is alerted to charges on the account because the account holder isn't a real person. Your institution is the initial victim, followed by those who had their personally identifiable information compromised. With SID fraud growing rapidly, this is a cause for not only concern, but (more importantly) attention and action.

Friend or foe?

Sophisticated criminals put a great deal of effort into creating convincing, verifiable personas. Once the fictional customer has embedded itself in your business, everything from the acquisition of financial instruments to healthcare benefits, utility services, and tax filings and refunds become vulnerable to synthetic identity fraud. Information attached to synthetic IDs can run several levels deep and be so complete that it includes public record data, credit information, documentary evidence and social media profiles that may even contain photo sets and historical details intended to deceive—all complicating your efforts to identity these fake customers before you do business with them.

Know the types of synthetic identities that may be entering your portfolio
There are three main ways criminals create synthetic IDs:

- Building a synthetic credit profile incrementally through applications and inquiries.
- Accessing legitimate accounts to exploit authorized user addition processes.
- Falsifying regular credit reporting agency updates via organized and illegitimate data furnishing schemes.

Stopping synthetic ID fraud — at the door and thereafter.

There are efforts underway in the market to collectively improve your ability to identify, shut down and prevent synthetic identities from entering your portfolio. This overall trend is great news for the future, but there are also near-term solutions you can apply to protect your business starting now.

While it's important to identify synthetic identities when they knock on your door, it's just as important to conduct regular portfolio checkups. Every circumstance has its own unique parameters, but the overarching steps necessary to mitigate fraud from synthetic IDs remain the same:

1. Identify current and near-term exposure using targeted segmentation analysis.
2. Apply technology that alerts you when identity data doesn't add up.
3. Differentiate fraudulent identities from those simply based on bad data.
4. Review front- and back-end screening procedures until they satisfy best practices.
5. Achieve a "single view of the customer" for all account holders across access channels—online, mobile, call center and face-to-face.

Using the right tools for the job.

In addition to the steps mentioned above, stopping these fake customers from entering and then stealing from your organization isn't easy—but with the right tools and strategies, it is possible. Here are a few of our top recommendations:

Forensics
Isolate and segment identities based on signals received during early account pathing, from both individuals and their device. For example, even sophisticated fraud networks can't mimic natural per-device user interaction because these organizations work with hundreds or thousands of synthetic identities using just a few devices. It's highly unlikely that multiple geographically separate account holders would share the same physical device.

High-risk fraud scores
Not all synthetic identity fraud manifests the same way. Using sophisticated logic and unique combinations of data, a high-risk fraud score looks at a consumer's credit behavior and credit relationships over time to uncover previously undetectable risk. These scores are especially successful in detecting identities that are products of synthetic identity farms. And by targeting a specific data set and relationships, you can maintain a frictionless customer experience and reduce false positives.

Analytics

Use a solution that develops models of bad applicant behavior, then compares and scores your portfolio against these models. There isn't a single rule for detecting fraudulent identities, but you can develop an informed set of rules and targeted models with the right service partner. Cross-referencing models designed to isolate high-risk identity theft cases, first-party or true-name fraud schemes, and synthetic identities can be accomplished in a decisioning strategy or via a custom model that incorporates the aggregate scores and attributes holistically.

Synthetic identity detection rules

These specialized rules consist of numerous conditions that evaluate a broad selection of consumer behaviors. When they occur in specific combinations, these behaviors indicate synthetic identity fraud. This broad-based approach provides a comprehensive evaluation of an identity to more effectively determine if it's fabricated. It also helps reduce the incidence of inaccurately associating a real identity with a fictitious one, providing a better customer experience.

Workstreams

Apply analytics to workstreams throughout the Customer Life Cycle, so you can address synthetic identities confidently:

- Credit risk assessment.
- Know Your Customer/Customer Identification Program checks.
- Risk-based identity proofing and authentication.
- Existing account management.
- Manual reviews, investigations and charge-offs/collections activities.

If your organization is like most, there's no time to waste when preventing synthetic identities from entering your portfolio. Criminals are highly motivated to innovate their approaches as rapidly as possible, and it's important to implement a solution that addresses the continued rise of synthetic IDs from multiple engagement points.

With the right set of analytics and decisioning tools, you can reduce exposure to fraud and losses stemming from synthetic identity attacks from the beginning and across the Customer Life Cycle.

Don't let your business become a victim of these synthetic identity fraudsters.
We can help you detect and mitigate these fake customers.

Ready to get started?

Experian
475 Anton Blvd.
Costa Mesa, CA 92626
T: 1 888 727 8330
www.experian.com