White paper

Synthetic identities: getting real with customers

Locate and minimize identity-based fraud with the right tools

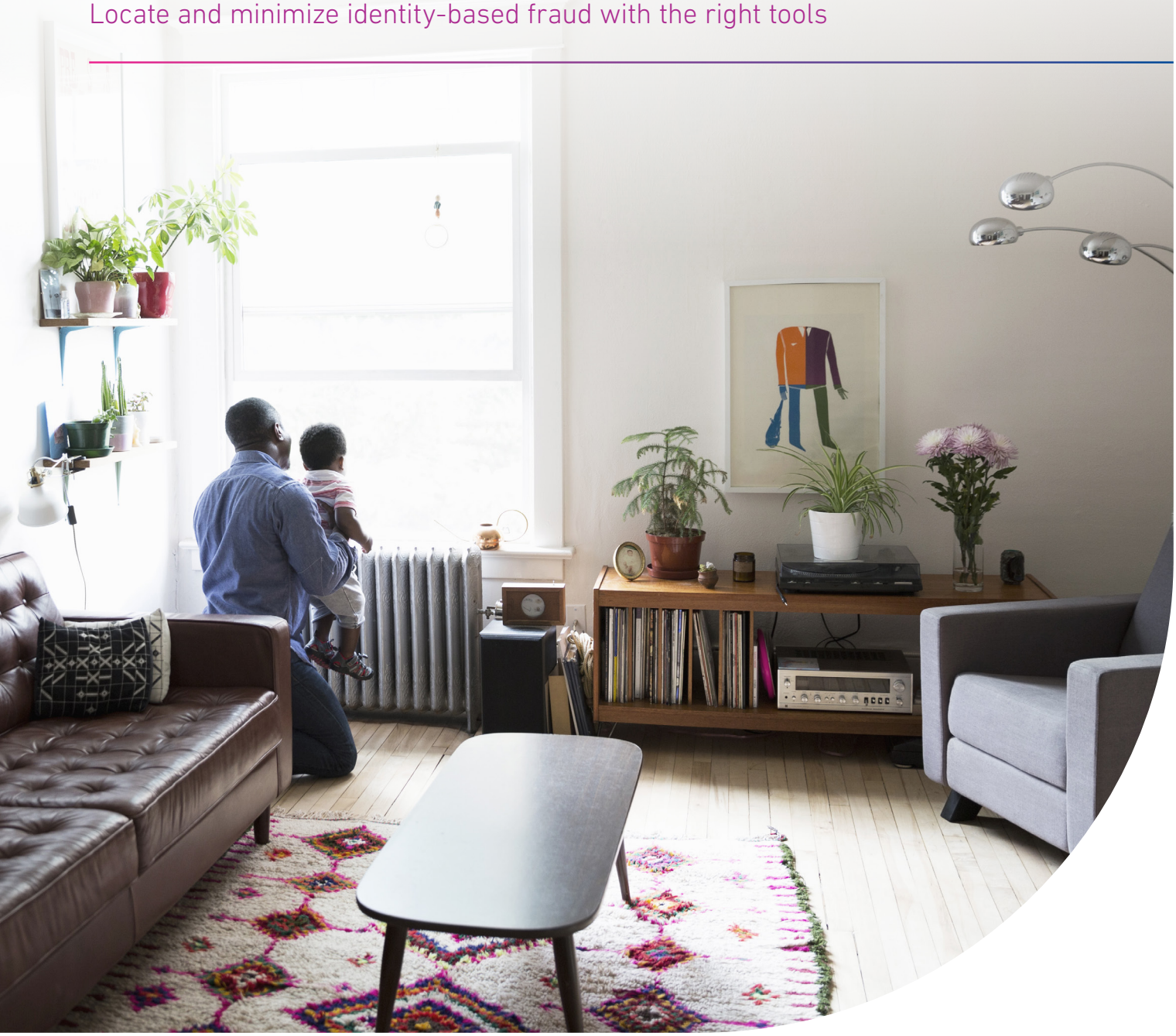


Table of contents

Introduction: Rise of the synthetics

Synthetic identities come from accounts not held by actual individuals, but by fabricated identities created to perpetrate fraud. And while analysts, institutions and service providers may not agree on the loss figure (although it's estimated in the billions annually), the impact of fraud is increasing significantly.

The term *synthetic identity* doesn't yet have a single, agreed-upon definition, but these identities are generally:

- Based on a Social Security number (SSN) or credit privacy number (CPN).
- A blend of fictitious and factual data, such as a mailing address from one individual combined with the telephone number of a second individual and the SSN or CPN of a third.

At the core, synthetic ID fraud involves a criminal combining real and fake information to create a new identity, which is subsequently used to open fraudulent accounts and make fraudulent purchases.

Sophisticated criminals put a great deal of effort into creating convincing, verifiable personas they can use to commit various types of fraud, ranging from acquisition of financial instruments to healthcare benefits, utility services, and tax filings and refunds.

Information attached to synthetic IDs can run several levels deep, including public record demographic data, credit information, documentary evidence and social media profiles that contain photo sets (and other historical details) intended to deceive.

How are synthetic IDs created?

There are three main ways criminals create synthetic IDs:

- Credit applications and inquiries that build a synthetic credit profile incrementally.
- Exploitation of authorized user processes to take over or piggyback on legitimate profiles.
- Data furnishing schemes to falsify regular credit reporting agency updates.

Alertless fraud makes losses harder to calculate

Synthetic ID fraud is thought of as a "victimless" crime, which is one reason it's difficult to combat. When a synthetic ID is used, no single individual is alerted to charges on the account, because the account holder isn't a real person. The institution providing services to the synthetic identity is the initial victim.

But this isn't always the case. Of grave concern is the fact that minors who may legitimately be issued SSNs that are being used to build synthetic IDs will find life as an adult much more challenging, and by default will be victims at some point. As these individuals become credit-active adults, they will find themselves subjected to heavy risk-based suspicion and a lack of positive and trusted identity verification, particularly with online and mobile services.

Synthetic ID fraud losses and charge-offs are often buried in, and diluted by, a larger pool of credit defaults.

Synthetic ID fraud can continue for an extended time, generating more profit for criminals, because lenders are often unaware of the level of synthetic infiltration in their portfolios. Losses are also easy to lump in with other delinquencies that lenders have come to forecast and accept as part of the standard cost of doing business — further obscuring the true cost of synthetic ID fraud. And synthetic ID fraud losses and charge-offs are often buried in, and diluted by, a larger pool of credit defaults. We've heard from many clients that current deltas between actual credit charge-offs compared with forecasted rates may in large part be due to synthetic identities being used to originate accounts.

Improved industry reporting and targeted analysis help assess costs

It's not easy to gauge exactly how much is being lost to synthetic ID fraud industry-wide. This is the result of inconsistent loss reporting, a lack of confirmable victims, and a lack of consensus on the exact definition of a synthetic identity to begin with. Regardless of overall losses, even when we analyze growth rates of only the most high-risk and obvious synthetics — the ones that charge off at toxic rates and were clearly created to perpetrate near-term fraud — Experian research shows that the problem grew more than 35 percent from 2015 to 2016, and is growing directionally in line through 2017.

As industry reporting becomes more accurate and awareness turns to operational detection and loss segmentation, we expect to discover that the costs of synthetic ID fraud are greater than initially believed. With the information currently available, Experian research shows that:

- Effective synthetic identity detection and fraud loss mitigation is often stymied by legacy first-party fraud policies and detection efforts. At Experian, we found that if an institution is chasing after the biggest number of losses, they are often chasing credit losses. In a recent study in which we eliminated small-dollar losses and focused on large-dollar losses with intent, we were able to increase the effectiveness of our synthetic identity model by 33 percent in the riskiest 1 percent.
- Average synthetic identity account losses are relatively high, but quite varied per institution. In looking at a subset of larger financial institutions, we found the average loss specific to synthetic ID fraud is approximately $6,000 per account, but ranges from $2,600 to $11,000 per account. This variance is attributable to factors such as addressable market populations, products or services available, customer acquisition channels, recovery opportunities, and level of sophistication and orientation to synthetic identity risk in identity proofing strategies.
- Bad rates within definitional high-risk synthetic identity populations also vary, with rates ranging from 8 percent to 22 percent (average bad rate of 11 percent) within a highly segmented population of likely synthetic identities. This can also be attributed to levels of sophistication in synthetic identity segmentation and any dilution of that segment with lesser-risk synthetic identities such as credit repair and emerging consumer/data quality cases.
- The good news — Additional risk ranking via targeted models allows for even further reduction in false positives, to a level approaching 2-to-1. This means actionable levels of account originations, for example, can be progressed through an attrition-based process with little impact to the good or true identities that meet some level of synthetic identity criteria as well.

The problem is substantial, and it's growing at an alarming rate. Yearly, as much as $300 million in charge-offs can be clearly attributed to synthetic IDs created for nefarious use. This loss figure pales somewhat in comparison to the billions in losses being attributed to synthetics overall (some of those figures are more defensible than others, and are some wildly and rather arbitrarily speculated to grab headlines, readership or business). But it does represent immediate risk that is more easily and realistically mitigated with targeted analytics that avoid the high false positive and good customer impact rates of other market offerings used to simply signal synthetic identity indicators. While the actual losses attributed to synthetic identities are clearly larger, perhaps three times or more, it's important to understand that not all of those identities are created equal, and they don't all display the same attributes. As institutions install tactical strategies to stem losses, detecting the more ambiguous synthetics may come at a higher cost to good customers who fall into the same categorical definition, often based on data quality and confidence levels.

Synthetic ID fraud average loss is approximately **$6,000 per account**.

Fake identities generate real losses

According to Aite Group, synthetic identity fraud will cause more than $800 million in losses to U.S. credit card issuers in 2017.

What's prompting criminals to shift to synthetic IDs?

Some methods of creating convincing identity profiles for nonexistent individuals require a lot of sustained work, and can involve coordination between multiple individuals within an illicit organization. By looking at what's motivating criminals to move to synthetic IDs, we can uncover some of the reasons the effort is worth it.

The data to create synthetic identities is available. A marketplace to exchange and monetize that data is expanding rapidly. The motivation and return on investment exists to perpetrate synthetic identity fraud. And, lastly, a lack of cohesive industry response to the problem is providing a relatively low barrier to entry for those incented to commit this type of crime.

The ingredients — the information is out there

The most readily apparent driver of the rise in synthetic ID creation is the high volume of data breaches (numbering in the thousands), the records compromised in those breaches (numbering in the billions) and the quality of data made available for nefarious use. Depending on the event, leaked information has included logins and passwords, credit card numbers, names, home and business addresses, SSNs, phone numbers, email addresses — even prescriptions and health records.

The utensils — online access makes fraud convenient

The advent of the dark web has provided centralized access to breached and compromised information. Proliferation of for-sale personally identifiable information (PII) has created a robust and lucrative channel for fraudsters looking for new cons; in fact, data is often available for sale on the dark web within hours of a major breach, and often priced at only a few dollars per record. Experian's CyberAgent® shows a 257 percent growth rate in the number of records compromised on the dark web from the first half of 2016 to the first half of 2017.

Inherently difficult to trace, new fraud sites are added to the dark web regularly, and many implement sophisticated user experiences, such as wish lists and shopping carts. These "fraud-on-the-go" sites greatly simplify the buyer's journey for individuals looking to illegally purchase PII, while the professional sheen further distances "shoppers" from the criminal reality of their intended purchase.

The recipe — Know Your Customer validation is basic

Years ago, the positive verification of a name, address, SSN and date of birth, for example, was considered a viable means to establishing confidence and trust in an identity presented at account origination. As most personally identifiable information is now — or should be considered — compromised, there is a risk of ongoing degradation in effectiveness for strategies anchored solely on that level of authentication. Compounding the challenge, the Social Security Administration recently began issuing SSNs randomly instead of in ranges consistent with region and date. This will further add ambiguity to the use of those numbers in synthetic identities, as a level of understanding (issuance date range and location) is now lost going forward. Far too many operational process points (whether during account origination or account management activities) continue to rely on such simplistic verification techniques, either because of lack of investment or a perceived lack of risk in the transaction itself. While risk-based verification or authentication certainly makes sense from a business perspective, it also opens paths of lesser resistance for the creation (and use) of synthetic identities in those processes deemed to be on the lower side of the risk spectrum.

The motivation — chip-and-signature frustrates crooks

It's important to consider the effect card-based protections, such as chip-and-signature form factors, are having on fraudsters. Also referred to as "EMV cards," debit and credit cards enabled with chip-and-signature technology create a physical roadblock for fraudsters historically engaged in

card skimming and counterfeiting, pushing them to look for new ways to gain access to available funds. Identity and card-not-present fraud schemes present an obvious and fruitful alternative pursuit. Synthetic identity creation and use lie squared within the spectrum of both types of schemes.

Aggressive and competitive lending practices leave gaps in identity fraud detection

Fraud detection and loss mitigation may often pale in comparison to the upside of high-volume market penetration and market share and the downside of overall credit risk. As such, fraud and identity management policies and practices often lag behind both marketing and credit policy layers of priority and focus. Logically speaking, therefore, it's safe to assume that the tradeoffs in less aggressive identity verification and risk assessment may be made in lieu of higher origination approval rates, market adoption, revenue and lower customer friction levels. Simply put, synthetic identity fraud schemes will continue to expose those tradeoffs.

Synthetic ID in a postbreach world

Of critical relevance is the fact that names, addresses, dates of birth and SSNs have been breached in combination. This provides an easy path for criminals to surgically target new combinations of data. Armed with an understanding of the actual associations across these PII elements, fraudsters can better navigate the best path to perpetrate fraud, whether identity theft, existing account takeovers, or the deconstruction and reconstruction of those elements to better create effective synthetics.

Using information such as birth dates and addresses in combination with SSNs, criminals can target new combinations of data to yield better results with lower risk of detection.

As an industry reliant on positive recognition of hundreds of millions of consumers and users, we must strive to continuously cultivate the broadest and most in-depth set of traditional, innovative and alternative data assets available in the marketplace. We must also enable the efficient and high-performing integration of that diverse set of identity attributes and intelligence to balance identity trust, identity risk, and customer or user experience.

Common synthetic ID scenarios

Fraud slows down systems, drives up costs and exploits the unsuspecting. Here are some real-world examples of the impact of synthetic IDs:

Auto

Auto lenders can experience fraudulent attainment of vehicles and subsequent charge-offs, but noncompliance with regulatory standards like Know Your Customer (KYC) and anti–money laundering (AML) can be even bigger concerns. When auto lenders' portfolios have been infiltrated with synthetic identities, compliance with KYC (and possibly other regulations) is seriously compromised.

Financial services

Synthetic IDs can be used to open a single account or a small number of accounts that immediately roll into a default or never payment status toward charge-off. Others can be used to acquire tradelines from multiple lenders, creating a fraudulent credit history. At a specific time, that combination of accounts may experience high line utilization followed by nearly simultaneous default, also known as a bust-out scheme. Lenders usually sustain additional costs as a result of the need to investigate and mitigate these threats, along with futile efforts to collect on a synthetic identity created to perpetrate fraud.

Public sector
In the public sector, synthetic IDs present a risk to the legitimate acquisition of services at the federal, state and local levels. These can range from tax refunds to utilities to other benefits afforded to citizens. As online and mobile access to such services grows, the use of synthetic identities becomes more appealing and fruitful to the fraudulently minded.

Healthcare
Aging healthcare infrastructures provide ready access points for criminals looking to gather highly useful data. Healthcare data is some of the most expensive on the dark web, because it can be leveraged as part of illegal prescription drug sales, or simply as a way to gain quality healthcare via fraud. Healthcare breaches can be harder to contain, since there is no single credit card to cancel and records may involve many levels of personal information. Healthcare organizations also stand to suffer reputational losses when services are provided to fraudulent identities.

What is a "bust-out" fraud scheme?

A bust-out scheme involves acting like an honest consumer long enough to maximize credit increases and new card issuances. The fraudster perpetrating the synthetic identity then vanishes, leaving behind a mountain of charge-offs and driving up costs for both financial institutions and consumers. This bust-out is more like a disappearance, in which the debt accumulated across a number of lenders is suddenly and unexpectedly abandoned.

Five steps to find and prevent synthetic identity fraud

Everything proceeds from the reliability of — and the level of available detail housed in — the origination data. You can apply existing technology to spot and segregate synthetic identities more easily during origination, and to authenticate customers with precision.

Although identities are sometimes flagged as synthetic during account origination, it's also important to conduct regular "portfolio checkups" to uncover synthetic identities that may have circumvented origination vetting.

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.

Not all synthetic IDs are created equal

Although it's hard to imagine a lawful reason why someone would want to create a synthetic identity, the goal isn't always retail or cash fraud. Synthetic IDs can be created for individuals who have no interest in fraud, but who would benefit from what they imagine to be a fresh start — like leaving a disastrous credit history behind.

Three types of synthetic identities

- **Bad —** Created to establish an identity and circumvent lag times and delays in establishing legitimate identity and data footprints.
- **Worse —** Created to "repair" credit, hoping to start again with a higher credit rating under a new assumed identity.
- **Worst —** Created to perpetrate fraud by opening various accounts with no intent to ultimately pay those debts or service fees.

While all these synthetic ID types are detrimental to the ecosystem shared by consumers, institutions and service providers, they must be segmented categorically and treated with proportional and effective methods to attrite them from an origination process or out of an existing portfolio of users or customers.

These steps can be accomplished via a consultative partnership that explores the following progressive discoveries:

1. Synthetic identity fraud exposure assessment and benchmarking to understand relative risk and opportunity to improve.
2. Customer data capture and authentication review to expose paths of least resistance for synthetic identity creation and/or usage.
3. Synthetic identity strategy review and design to ensure targeted detection and workflow treatments specific to the nuanced risk and attributes surrounding a synthetic ID.
4. Data furnishing assessment to determine what role your organization can play in reducing the proliferation of synthetic IDs.

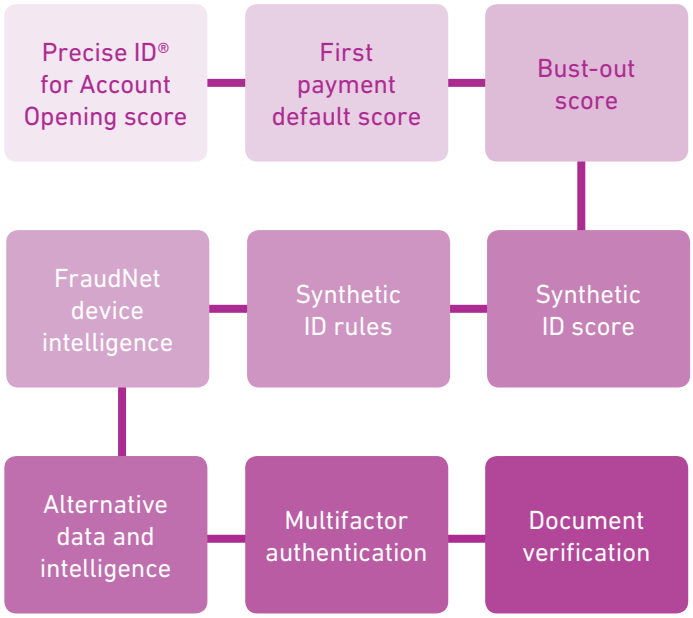
There are also efforts underway between large financial services organizations and many governments (including the United States) to collectively improve your ability to identify and shut down synthetic identities. This overall trend is great news, but there are also near-term solutions you should apply to your own portfolios to protect your investment, starting now.

Applying the right technology in the right places

In addition to the steps already recommended for resolving synthetic IDs in your organization, you can also apply specific protective approaches to corresponding points in your workflow and portfolio structures.

Layered fraud detection and risk mitigation

Solutions can be bundled in various combinations to address the unique needs of your business most effectively.



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. In reality, it's highly unlikely that multiple, geographically separate account holders would share the same physical device.

Analytics

Use a solution that develops models of bad actor 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.

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.

Prescriptive approach and considerations

Synthetic identity detection and loss mitigation require a layered approach that must be applied at both account origination and account or portfolio management process points. Additionally, a targeted set of step-up or additive authentication methodologies should be accessible when dictated by initial assessment of potential synthetic identity risk. Institutions should consider the appropriate capabilities in applying a layered approach to synthetic identity detection and risk segmentation across the Customer Life Cycle. Comprehensive decisioning can be obtained through more sophisticated strategies that blend scores, underlying attributes and conditional exceptions based on orchestration that determines when to invoke what combination of such capabilities and data assets.

Definitions and reporting

Apply best practices to inform others within and outside your organization of the importance of combating synthetic identity fraud and improved reporting techniques.

Consortium data

As definitions of synthetic identity become more consistent and operational "confirmation" of them occurs, the opportunity for consortium-level sharing of such information gains value. While many such consortiums, or "black lists," show initial value to user institutions, they often fall victim to aged data and inconsistent information or categorization, and therefore a degraded level of trust. In the case of synthetic identities, however, value does exist if used in combination with other critical techniques.

Account origination	Account- or portfolio-level management	Step-up authentication
Identity element validation and verification	Identity element linkage and velocity analysis and attributes	One-time password
Identity element linkage and velocity analysis and derivative attributes and score	Synthetic identity risk score	Alternative data and risk attributes and scoring
Identity risk score	Bust-out fraud score	Remote document validation and verification
Synthetic identity risk score	Device intelligence and risk assessment	Social Security Administration — consent-based Social Security number verification (CBSV)
First payment default score		Biometrics and behavioral data
Bust-out fraud score		
Device intelligence and risk assessment		

Multifactor/Step-up treatment
Multifactor authentication is based on the premise that an unauthorized person can't provide the same variety of proof elements as an actual consumer. This makes it easier to see that a consumer's identity hasn't been established with certainty, preventing potential fraud. Supplying consumers with a one-time password (OTP) is one increasingly popular example of strengthening the authentication process, especially for high-risk or high-value transactions.

Document validation and verification can also be effective in further vetting potential synthetic identities. Direct access to Social Security Administration data is available today as a viable option during more aggressive identity proofing of potential synthetic identities. That said, much work remains to be done in making current procedural options more viable for higher-volume, real-time checks and reducing cost and customer friction by making it easier to attain permissible purpose and consent.

What does success look like?

Leading solutions will have identifiable capabilities for stopping synthetic ID infiltration. Some attributes of the successful implementation of antisynthetic ID technology:

- Traditional and alternative data combined at account opening and account management process points.
- Effective policies and documented procedures.
- Risk segmentation strategies and workflow design.
- Targeted scores and attributes for use at account opening process points and portfolio-level monitoring and alerts.
- Fewer false positives, improving operational efficiency and reducing resources needed for investigation.
- Future-ready synthetic identity model and decisioning attributes, including key performance indicators, continue to fine-tune the solution.
- Step-up authentication options orchestrated and delivered via synthetic identity workflows.
- Consistent reporting and feedback mechanisms for highly suspected or confirmed synthetic identities.

What needs to improve?

The path to success in mitigating the effects of synthetic identities isn't always clear, but there are signposts of improvement we can use to ensure we're headed in the right direction:

- Expanded access and consumer consent options to better vet SSN, name and date of birth associations.
- Industry and cross-market agreement and standardization of synthetic identity definitions and confirmation processes.
- More granular reporting mechanisms particular to synthetic identities for credit reporting agency data furnishers.
- More critical mass of confirmed synthetic identities for use in model and strategy design.
- Less fractured or more consolidated consortium data assets with respect to known or highly suspected synthetic identities and elements.
- More consistent and foundational baseline levels of identity proofing and authentication across all application and identity management channels and access points.

If your organization is like most, there's really no time to waste when addressing synthetic IDs. 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 across the Customer Life Cycle and across channels.

Experian
475 Anton Blvd.
Costa Mesa, CA 92626
T: 1 888 414 1120
www.experian.com

10/17 • 2000/1302 • 1145-DA