Middesk

How to combat synthetic identity fraud in business onboarding

Contents

Introduction

Synthetic identity fraud is the fastest-growing financial crime in the U.S., responsible for billions of dollars in annual losses across industries. Unlike traditional identity theft, synthetic fraudsters create false identities by combining real and fabricated information such as addresses, tax identification numbers (TINs), and website URLs. These synthetic identities, which can be personal or business identities, can then be used to open fraudulent business accounts, secure loans, make high-value purchases, or establish credit lines. In effect, they pose a significant risk for financial institutions, fintech companies, and e-commerce platforms of all sizes.

This type of fraud is particularly difficult to detect because synthetic identities often appear legitimate, behaving like real people or businesses for months or even years. For example, fraudsters might make small, on-time payments to build up their credit before taking out a large loan and disappearing before their creditors notice they've defaulted.

Given the evolving sophistication of synthetic fraud networks, traditional Know Your Business (KYB) and Know Your Customer (KYC) methods of risk mitigation often aren't enough.

Rather than simply meet minimum compliance standards, financial institutions, fintechs, and e-commerce companies must adopt layered verification models, leverage alternative data, and implement AI-driven fraud detection systems to protect their businesses from the threat of synthetic identity fraud.

In this guide, we lay out an integrated, multi-layered approach to detecting and preventing synthetic identity fraud in business onboarding. Drawing from the latest techniques of bad actors and the most current technology available for proactively fighting back against fraud, we present an actionable framework that financial institutions and e-commerce companies can use to streamline verification processes and modernize their fraud prevention systems.

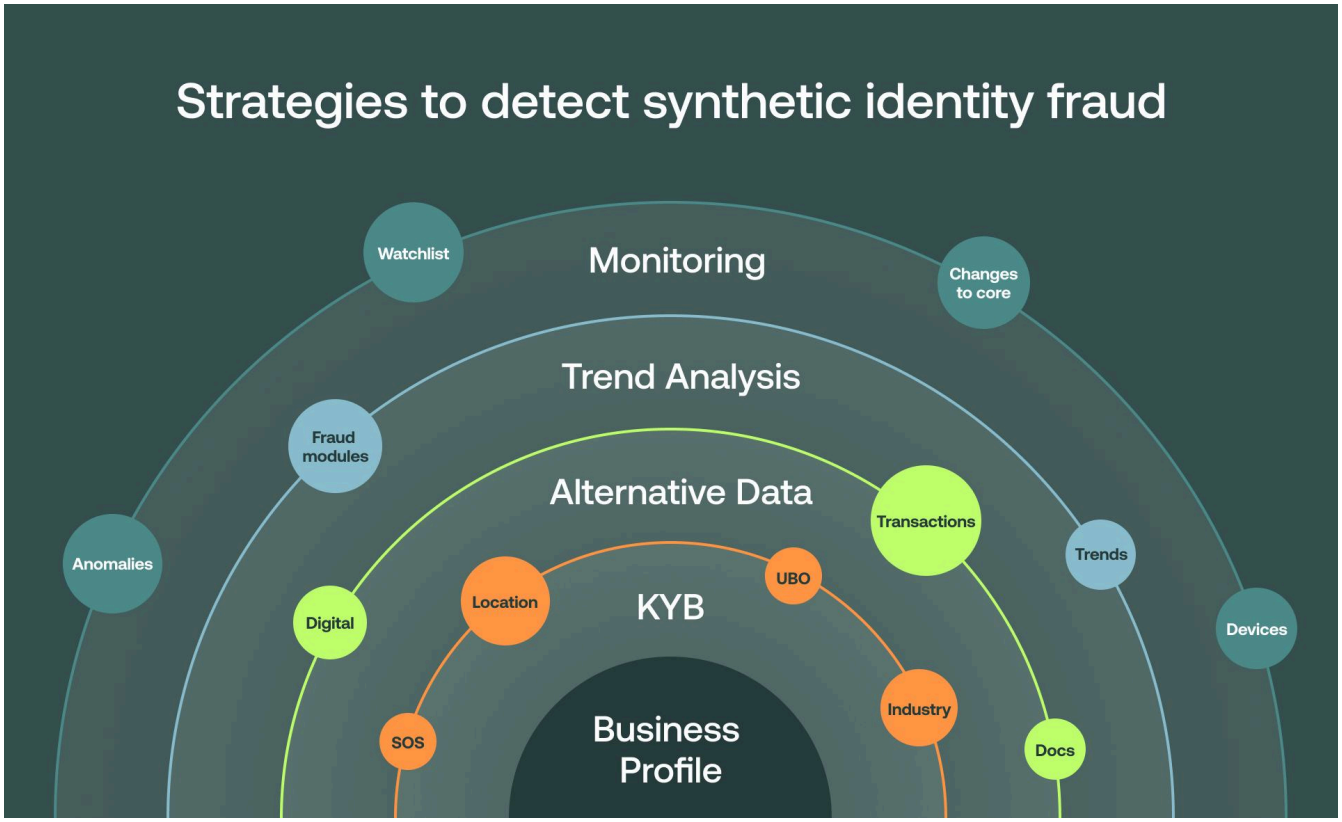
The high cost of fraud for financial and e-commerce businesses

The financial services and e-commerce industries bear the brunt of synthetic identity fraud due to their high transaction volumes, rapid onboarding processes, and digital-first business models. Fraudsters target these sectors because they often prioritize growth at the expense of risk management.

Key risks of synthetic fraud

- Operational strain: Fraud investigations require extensive time and resources from analysts, legal teams, and technical experts. Many businesses struggle to scale fraud prevention efforts as synthetic identities become more sophisticated.
- Revenue loss: Once fraudsters are able to escape with a loan they will never repay, financial institutions often have no recourse for recovering funds. For e-commerce businesses, fraudulent chargebacks contribute to rising payment processing costs and account closures.
- Reputational damage: The long-term consequences of synthetic fraud include eroded customer trust, regulatory penalties, and jeopardized banking licenses or partnerships. When businesses fail to detect fraudulent activities, they risk being perceived as insecure or unreliable by investors, partners, and consumers.

To stay ahead of synthetic fraud, financial services and e-commerce companies must move beyond baseline verification techniques.



By leveraging the more comprehensive data sets that are readily available today, these companies can take a more proactive approach to fraud prevention to reduce financial losses, improve compliance, and enhance customer trust.

In the following pages of this guide, we'll show how companies can enhance the sophistication of their customer onboarding, from business verification to leveraging alternative data sources and eventually integrating trend analysis and monitoring into the risk management process.

1. Solidifying business verification

Key vulnerabilities:

- Fraudsters exploit loose incorporation regulations to create shell companies.
- Multiple businesses registered to the same address can be a red flag.
- Lack of historical financial activity or transactional records suggests synthetic operations.

At the foundation of fraud prevention is the verification of a business's legitimacy. Traditional KYB checks, such as verifying business registration details, EIN/TIN matching, and ownership structures, are an essential first step toward detecting sophisticated fraud attacks.

> In December 2021, Michael Griffin, the leader of a synthetic identity fraud ring, was sentenced to prison for orchestrating a scheme that defrauded multiple banks. The operation involved creating fictitious identities to open bank accounts and secure loans, resulting in significant financial losses. This case underscores the growing threat of synthetic identity fraud in the financial sector. Learn more about this case at the IRS website.

Business identity verification is often compromised by fraudulent actors exploiting weak incorporation regulations to register shell entities with minimal scrutiny. For example, bad actors might provide false documents and utilize mail-forwarding services or virtual addresses to obscure their true origins. Many fraudsters take advantage of states with lenient business formation laws, making it easier to set up fake companies that appear legitimate on paper.

Fraud detection is further complicated by the increasing use of nominee directors — individuals hired to act as a company's registered officer without having any real connection to its operations. To combat this, regulators and businesses should implement more rigorous ultimate beneficial ownership (UBO) verification and cross-reference applicants with global watchlists and adverse media databases to detect high-risk entities.

Best practices for business verification

- Verify businesses against multiple third-party and government databases.
- Implement automated EIN cross-checks to flag duplicate registrations.
- Use AI-powered analytics to detect anomalies in business registration patterns.
- Strengthen UBO verification and monitor nominee director patterns.

2. Leveraging alternative data

Many synthetic fraud schemes evade detection by exploiting weaknesses in standard KYB processes. Fraudsters use synthetic identities to create business bank accounts, obtain loans, and process fraudulent transactions — all under seemingly legitimate business credentials.

Red flags in business identity verification:

- Mismatched business and personal details
- Fake or missing registration numbers
- False or missing addresses
- Lack of a proper privacy policy
- Difficulty identifying ultimate beneficial owners (UBOs)
- Rapid and illogical transactions
- Poor or missing transaction documentation
- Post-audit tampering
- Use of registered agent addresses as primary business locations
- Frequent business name changes within a short period
- Patterns of duplicate contact info used across multiple accounts

One challenge in strengthening KYB checks is the overreliance on one-time identity verification methods. Traditional checks focus on business filings, tax records, and corporate structures, but use out-of-date information and/or fail to analyze the legitimacy of an entity's activity over time. A more effective approach includes ongoing validation through network analysis, transactional monitoring, and real-world activity verification.

> We've seen fraudsters blend real and fake information so seamlessly that they pass traditional KYB. The key is not just checking business existence, but verifying the legitimacy of activity behind that entity.

Jules Mei
Product Ops at Middesk

Additionally, KYB processes should incorporate behavior-based information and device intelligence to detect inconsistencies in login locations, IP addresses, and device usage. Financial institutions and e-commerce companies have successfully leveraged AI-driven behavioral analysis to uncover synthetic identities that use identical device fingerprints across multiple applications, revealing fraud rings operating at scale.

To combat synthetic identity fraud, companies must look beyond static identity checks and incorporate alternative data sources. For example, Address Risk Insights, included within Middesk's core Verify product, leverages an extensive, proprietary database of over 40,000 registered agents across the U.S., authoritative U.S. government business data, international address data, and high-quality alternative data to provide deeper risk analysis using alternative data, including:

- **Risk-based verification:** Assess address legitimacy by validating its existence, determining whether it is U.S.-based or international, and confirming deliverability to verify a real business location.
- **Registered agent detection:** Cross-reference addresses with our database of known registered agents to flag those frequently linked to fraudulent activities.
- **Mailbox designations:** Detect high-risk mail services such as private mailboxes, PO boxes, and virtual addresses using postal service data.
- **Location frequency:** Evaluate how many businesses are associated with a given address to uncover potential fraud indicators.

Additionally, ongoing analysis of social media activity, industry affiliations, and vendor transactions can offer insights into whether a business is engaging in genuine commercial activity or merely existing on paper. These additional data points can include:

- **Transactional history:** Evaluating patterns of legitimate vs. suspicious financial activity
- **Device and geolocation data:** Identifying shared devices or unusual IP addresses
- **Website and digital footprint analysis:** Assessing inconsistencies in online business presence

The reality is that synthetic businesses often lack meaningful engagement with suppliers or customers. If any customers are demonstrating little-to-no activity across these different areas, it can be a strong signal of fraudulent intent.

> In May 2024, the Federal Trade Commission (FTC) took action against payment processing company BlueSnap, Inc., for knowingly processing payments for fraudulent companies. The defendants agreed to a $10 million settlement. Learn more about the case at the FTC website.

Best practices for leveraging alternative data

- Incorporate AI-powered behavioral analysis into verification processes.
- Cross-reference applicants with industry databases and transaction history records.
- Flag businesses with no verified supplier or customer relationships.

3. Analyzing trends and monitoring behavior

Synthetic identity fraud techniques continue to evolve as fraudsters develop new techniques to bypass traditional verification methods. To stay ahead of new threats, financial institutions must adopt trend analysis and behavioral monitoring, which includes leveraging AI and machine learning to track anomalies and predict fraudulent activities before they cause financial harm.

Effective trend analysis involves monitoring account activity over time to detect suspicious behavioral patterns. For example, a business that suddenly shifts from low-risk transactions to high-volume, high-risk transactions should trigger an alert. Additionally, fraud networks often use the same fraudulent tactics repeatedly, making it crucial to compare new applicants to previously identified fraud patterns.

Financial institutions and e-commerce should leverage:

- **Machine learning models** to detect anomalies in financial activity.
- **Real-time transaction monitoring** to identify suspicious banking behaviors.
- **Cross-referencing historical fraud indicators** to predict emerging risks.

Even businesses that initially pass identity verification checks can become fraudulent over time. This makes continuous monitoring and real-time alerting a crucial component of an effective fraud prevention strategy.

Fraudsters often engage in transaction “layering," where small amounts of money are moved through multiple accounts to avoid detection. By implementing real-time transaction monitoring and machine learning models that assess risk based on changes in transaction behavior, financial institutions and e-commerce companies can proactively identify suspicious activity before taking significant losses.

Real-time monitoring ensures financial institutions can detect:

- Sudden address or phone number changes
- Unusual transaction spikes or rapid fund withdrawals
- Connections to entities appearing on watchlists

The bottom line

Fraud is evolving — fraud prevention must evolve, too

Organizations that rely on baseline verification methods are more vulnerable to fraudsters who exploit regulatory loopholes and gaps in digital identity validation. A proactive, intelligence-driven fraud prevention strategy integrates real-time monitoring, alternative data analysis, and AI-powered risk assessment tools to detect synthetic fraud before it results in financial loss.

The path forward

- **Invest in continuous monitoring:** Fraud prevention doesn't stop after onboarding. Real-time transaction monitoring and ongoing risk assessments can help businesses stay ahead of evolving fraud schemes.
- **Enhance identity verification with alternative data:** Cross-referencing traditional identifiers with behavioral analytics, geolocation data, and digital footprints strengthens fraud detection capabilities.
- **Prioritize automation and AI-driven fraud detection:** Machine learning models that detect anomalies in user behavior and transactional patterns allow for more accurate, scalable fraud prevention.
- **Strengthen collaboration across industries:** Sharing fraud intelligence across financial institutions, fintechs, and e-commerce networks improves collective fraud detection and mitigates broader systemic risks.

Middesk is making it possible for businesses to protect against sophisticated synthetic fraud schemes while still giving their legitimate customers a seamless onboarding experience. This stronger, more secure onboarding workflows provides:

- **Seamless KYB and identity verification** that goes beyond basic compliance checks
- **Real-time fraud monitoring** to track suspicious behaviors before they escalate into financial losses
- **Automated review processes and risk scoring models** to detect synthetic fraud patterns at scale

About Middesk

At Middesk, our mission is to make it easier for businesses to work together by providing instant access to the data, documents, and insights needed to onboard and transact in the global economy. Since 2018, we have been a leading disruptor in the business identity market. We have over 400 customers across financial services, and were early to market with a KYB solution that has given us a unique view of this market and how it has evolved. Financial institutions from payment providers to tech-first neobanks, to top national institutions trust Middesk to optimize their business identity workflows.

Our best-in-class business identity platform provides access to complete, up-to-date information that financial services institutions and fintechs need to make educated decisions about their customers and facilitate rapid onboarding and transacting. Our vision is that every company can instantly gain access to all the data, products, and services they need to establish and grow their business with ease. Middesk came out of Y Combinator, is backed by Sequoia Capital and Accel Partners, and was recently named to Forbes Fintech 50 List and cited as an industry leader in business verification by digital identity strategy firm, Liminal.


Middesk