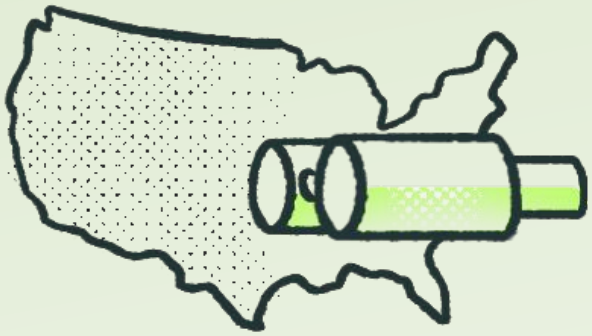
Middesk



Using data to defend against shelf and shell companies

Contents

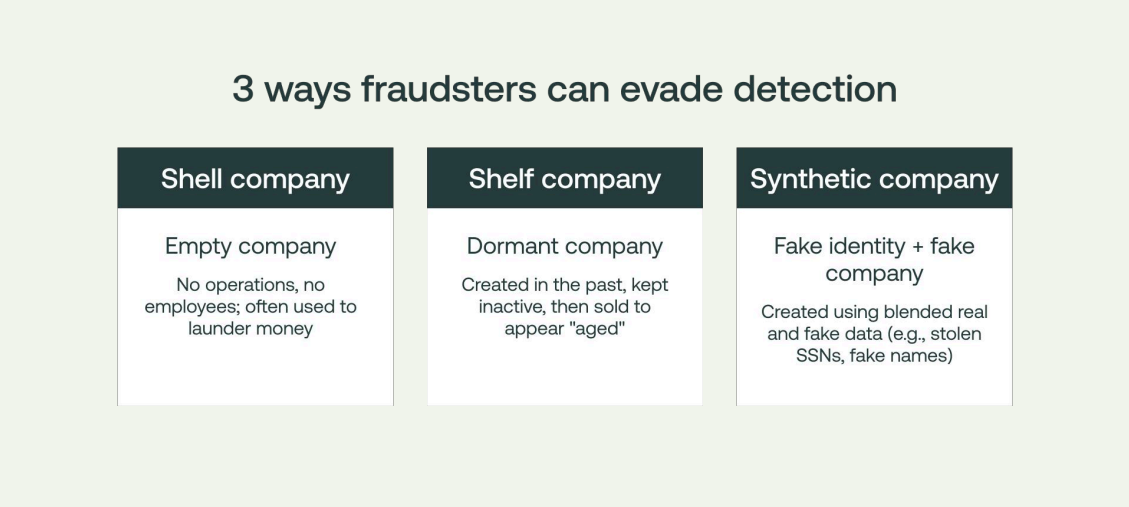
Introduction

Recent changes to federal regulations have made it even harder for banks, fintechs, and marketplaces to verify who they're doing business with. In March 2025, the Financial Crimes Enforcement Network (FinCEN) announced it would no longer require U.S. companies and certain foreign entities to report beneficial ownership information through the Corporate Transparency Act. This means institutions are more reliant than ever on their own systems to vet and verify business customers.

As Middesk CEO, Kyle Mack, noted in an op-ed for American Banker, this policy shift increases pressure on state governments and private businesses alike to close the gaps left by inconsistent federal reporting. But there's another growing threat lurking beneath the surface: the use of shelf, shell, and synthetic companies as tools for fraud.

"These aren't abstract entities," said Jules Mei, Product Operations at Middesk. "They're sophisticated fraud tools being used right now to get around standard checks and move illicit money. And unfortunately, they're effective."

This guide explores how modern risk teams can use deeper data signals to spot fraud early — without adding friction for legitimate businesses.



What are shelf, shell, and synthetic companies?

Fraudsters are using increasingly sophisticated strategies to create companies that are designed to deceive. These can come in three forms you should know about:

- Shell companies are businesses with no real operations or employees. They exist only on paper and are often used to launder money or obscure ownership.
- Shelf companies are dormant entities formed years ago and later sold to fraudsters who exploit their age and clean credit history.
- Synthetic companies blend real and fake data — such as stolen SSNs or EINs — to create entirely fabricated businesses capable of passing onboarding checks.

“These tactics are being used together now, not just in isolation,” said Mei. “Fraudsters use synthetic data to create fake identities, then use those to register shell or shelf companies.”

By masking shell and shelf companies with fraudulent data, bad actors can often evade detection by point-in-time KYB checks.

Why traditional KYB falls short

Traditional KYB programs were built for a different era — one where verifying that a business was legally registered was often enough. But shelf, shell, and synthetic companies have exposed the limits of this approach.

Standard KYB programs typically verify registration details like:

- Business name
- Incorporation date
- EIN or tax ID
- Basic ownership information

While useful, this snapshot fails to capture whether a business is actually operating. Fraudsters exploit this blind spot by registering entities that check all the boxes on paper but show no signs of real-world activity.

Red flags traditional KYB often misses:

- Inconsistent identity information
- Use of registered agents to obscure true ownership
- No employees or payroll
- PO boxes or virtual addresses

"Everything might look great on paper, but the operations are either fake or non-existent," Mei pointed out. And that's the real gap. Traditional KYB wasn't designed to detect operational risk — but that's exactly where today's fraudsters hide. It's no longer enough to verify registration details. To stay ahead, you need to understand whether a business is *actually active*.

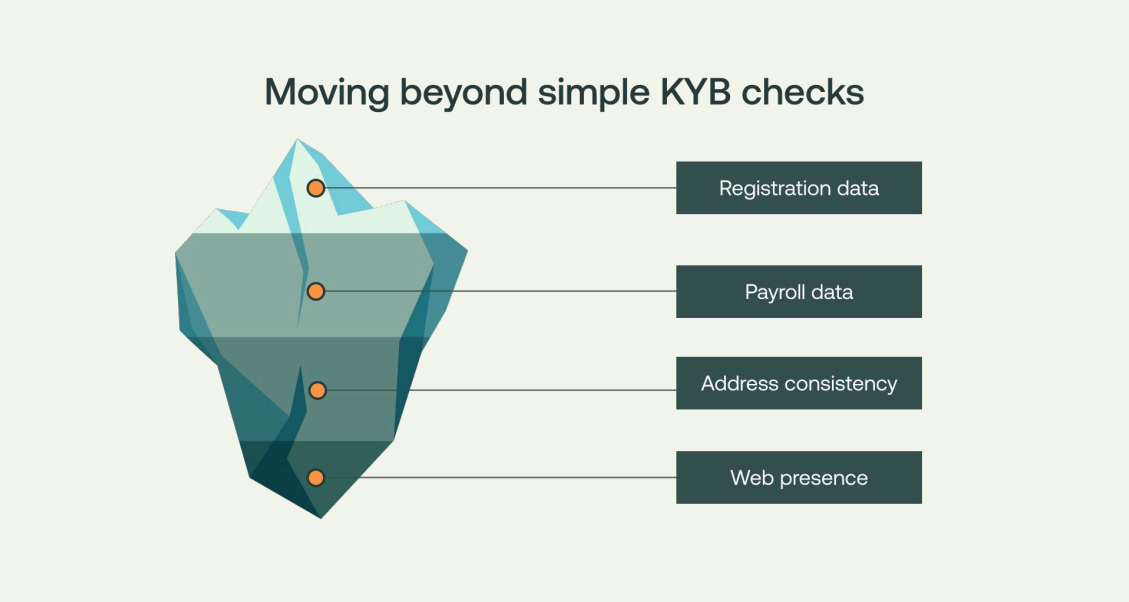
The data fraudsters can’t fake

Fraudsters can fake documents, but real-world business activity is much more difficult to imitate. Today’s KYB has to look beyond static incorporation forms and tap into data that shows whether a business is truly active.

Key data signals:

- **Network analysis**: Are there shared owners, addresses, or agents with known fraud cases?
- **Payroll data**: Do they have real employees? Does payroll volume match their claimed industry?
- **Address consistency**: Is it a PO box? A freight port? Or a legitimate office?
- **Web presence**: Do they have a website? Any traffic, reviews, or listings? Is the domain age consistent with their registration?

“Web data and payroll signals help tell the real story,” Mei explained. “Does this business behave the way you’d expect for its size and industry? Are there employees, reviews, and online activity that align with what’s on the paperwork?”

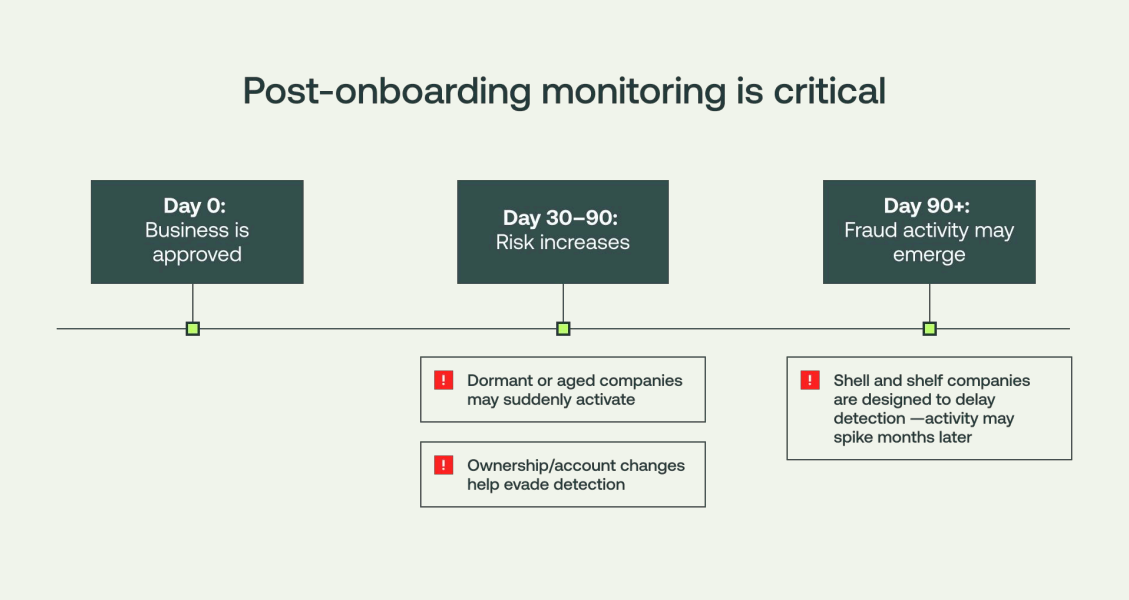


Why post-onboarding monitoring matters

Even with smart onboarding checks, some fraudulent businesses will make it through. That's why monitoring behavior over time is essential.

Signs of risk post-onboarding:

- Sudden ownership changes
- Circular fund movements
- Spikes in activity from previously dormant accounts



"These companies are designed to delay detection," said Mei. "Everything might look clean during onboarding, but once they've cleared your checks, the fraudulent activity begins."

These behaviors often emerge 30–90 days after onboarding — well after traditional risk checks stop. Catching them early can prevent losses, regulatory exposure, and reputational damage.

Building a smarter KYB framework

To defend against modern fraud techniques, risk teams need to move from one-and-done checks to a full lifecycle approach.

Your KYB process should include:

- **Authoritative data**: Government filings, DBAs, licensing info
- **Alternative data**: Web presence, reviews, traffic patterns
- **Network analysis**: Entity linkages across owners, addresses, and agents
- **Post-onboarding signals**: Ownership updates, payment activity, operational shifts

"Your KYB program should work like a radar, not a checkbox," said Mei. “You need visibility into what’s changing — who’s connected to whom, how activity is evolving, and what risk looks like over time.”

How to design your fraud detection program

Start with a KYB audit	Rethink your risk signals	Assemble the right team
Are you only verifying business registration?	Are you monitoring ownership changes, activity spikes, and shared agents?	Risk, compliance, and fraud teams: Align on smarter checks
Are you checking for real-world signals like activity, ownership, and connections?	Can your systems surface patterns across connected entities?	Product and data teams: Automate real-world signal detection

Purpose-built business verification prevents fraud in a deregulated environment

The combination of looser federal BOI reporting and increasingly complex fraud strategies means financial services companies must rethink how they verify businesses. Relying solely on incorporation data isn't enough.

The good news: The data to fight back already exists. Payroll signals, domain intelligence, and network relationships all provide powerful ways to detect fraud before it causes harm.

By layering authoritative and alternative data, investing in post-onboarding monitoring, and using tools that surface hidden connections, risk teams can protect their companies without slowing down legitimate business customers.

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 the Forbes Fintech 50 List and cited as an industry leader in business verification by digital identity strategy firm, Liminal.

See how Middesk can level-up your onboarding process.

Schedule a demo


Middesk