Why B2B Fraud Keeps Winning and What We Can Do About It

By: Andrew J. La Marca, Senior Director of Risk and Fraud Operations, Dun & Bradstreet

Originally published in the Credit Research Foundation's publication, Perspective by CRF (Q3 2025)

Business-to-business fraud is a topic I've spent years immersed in, and I can tell you — it's not just persistent, it's evolving.

What makes it so compelling to bad actors is how easy it is to exploit. It's shockingly simple to compromise a business registration, impersonate an owner or officer, and fabricate documentation that looks legitimate. And once that façade is in place, fraudsters can operate with surprising freedom.

Unlike the consumer credit space, the B2B environment isn't universally regulated. Outside of financial institutions or highly regulated industries, businesses aren't required to perform Know Your Customer (KYC) or Know Your Business (KYB) checks. In fact, some organizations are willing to accept fraud losses if it means preserving a frictionless customer experience.

Add to that the challenge of law enforcement, and how difficult it can be to pursue perpetrators domestically and internationally. All of this creates a perfect storm: low barriers, high reward, and minimal risk for fraudsters.

B2B Fraud Deserves More Focus

One of the biggest pain points in B2B fraud is the inconsistency in how businesses treat it. Consumer fraud gets the headlines, the airtime, and the public awareness. Business fraud? Not so much. That lack of visibility translates into a lack of urgency — and a lack of investment in prevention.

Cross-border fraud introduces even more complexity. Language barriers, inconsistent data standards, and varying levels of fraud awareness across regions make it difficult to detect and respond effectively. Some firms lump all types of fraud into a single category, which obscures the nuances and makes it harder to build targeted defenses.

Artificial intelligence is transforming the fraud landscape on both sides of the fight. Fraudsters are using AI to scale their operations and create realistic documents, websites, and even synthetic identities with alarming ease. The ability to mimic legitimacy has never been more accessible.

But AI isn't just a threat; it's also a tool for defense. Predictive analytics, anomaly detection, and real-time monitoring powered by AI can help businesses stay one step ahead. The key is balance. Too much automation without human oversight can be dangerous.

While AI is powerful for helping to detect fraud, it's not a silver bullet. Automation can streamline processes, but it can also introduce blind spots. You need humans to monitor, interpret, and intervene when necessary. Fraud detection is not a "set it and forget it" operation.

Fraud detection still requires human judgment, especially when it comes to interpreting signals and making decisions. Humans are assets in this fight, and we need to keep them in the loop.

Why You Need to Be Cautious about Business Registration Data

One of the most overlooked vulnerabilities is at the point of business registration. In the U.S., forming a legal entity starts with a state registrar. But not all states verify the information they receive. Fraudsters exploit this by hijacking existing companies or creating new ones with false data. Once registered, that entity

becomes a "proof of right" for credit applications, purchases, and more.

B2B companies need to be extremely vigilant about checking for signs of potential fraud. When you examine state registrar data, pay particularly close attention to:

- Entity verification: Is the business legally registered? Is it active or dissolved?
- Address validation: Is the business operating from a commercial location or a residential one?
- Ownership clarity: Are the listed officers or owners consistent with other records? And are they legitimate person(s)?
- Filings: Pay attention to the velocity or lack of velocity in annual filings if required.
- EIN confirmation: Does the business have a valid Employer Identification Number?

Entity type is also important. If you understand the legal structure of a business, you can better scrutinize the data and more accurately assess the potential for risk.

Remember that with sole proprietorships, the owner is personally liable, so verify their identity carefully. With LLCs and corporations, liability is limited, meaning collections may be restricted to corporate assets. In partnerships, because risk exposure varies by partner, you should be clear about who's on the hook for what.

To close this gap, we need universal alignment on key actions. Registrars should verify data before filings go public. That data should be updated regularly, standardized across states, and shared with the broader business ecosystem via real-time access. And every organization offering credit, goods, or services should adopt a consistent approach to fraud prevention — no shortcuts.

The Power of Networks

Data-sharing networks and consortiums are essential. At Dun & Bradstreet, our D&B® Fraud Risk Network enables businesses to share intelligence and receive insights in return from a team of Certified Fraud Examiners.

But it's not just about joining; it's about vetting. Look at the hosting organization, their data standards, and their privacy policies. Conduct a proof of concept to ensure the network delivers value to your organization and the ecosystem.

Even anonymized sharing can make a difference. You don't have to reveal proprietary data. Just signal that an entity exhibits risk characteristics. That alone can help others avoid falling victim.

Saying "fraud is a risk" isn't enough. You need to classify it. Is it business identity theft? Misrepresentation? Synthetic entities? First payment default? These distinctions matter. Once you've classified your risks, you can build frameworks to mitigate them.

Centralizing your data is crucial. Scattered data makes it almost impossible to model, govern, or audit effectively. Integration gives you transparency and the ability to act.

Training and Business Culture Matter

Fraud prevention isn't just a job for the risk team. It's everyone's responsibility. Just like cybersecurity, every employee needs to be trained to recognize and report suspicious activity. Awareness empowers people to act, and it protects them as consumers too.

Most B2B fraud comes from external actors. But internal threats exist too, through schemes such as vendor

invoicing orchestrated by rogue employees. These schemes often involve creating fake businesses and rerouting funds. While less common, they're no less damaging.
Fraud looks different depending on the industry. In finance, scams like pig butchering are rampant. In auto and heavy equipment, we see identity theft and fictitious employers. In insurance, misrepresentation and third-party fraud are common. Each vertical faces unique challenges, and data management strategies must adapt accordingly.

Larger enterprises typically have more sophisticated fraud programs, as well as established audit, controls, training, and monitoring. SMBs, especially startups, often lack the resources. Their focus is on growth, not governance. But that makes them vulnerable. Over time, SMBs can adopt more robust practices, but the journey starts with awareness.

As real-time payments and cryptocurrencies gain traction, governance becomes even more critical. Businesses must establish standards for quality, security, and monitoring. They need to collect the right data — like email addresses on digital applications — and track customer behavior over time. Understand what's normal, then act when things deviate.

The bottom line is that fraud is evolving, and so must we. Avoiding and protecting your business from it won't happen just with technology. Companies need to strengthen and enhance their strategy, collaboration, and culture. Whether you're an enterprise or an SMB, in finance or retail, the principles remain the same: know your risks, manage your data, and never stop learning.

About the Author

Andrew J. La Marca, CFE, CAMS, is a seasoned leader in global fraud prevention and compliance, with more than 15 years of experience spanning Capital One, Ally Financial, and Dun & Bradstreet. He is recognized for driving pivotal initiatives that reduce fraud risk, ensure regulatory compliance, and enhance data integrity across complex, global operations.