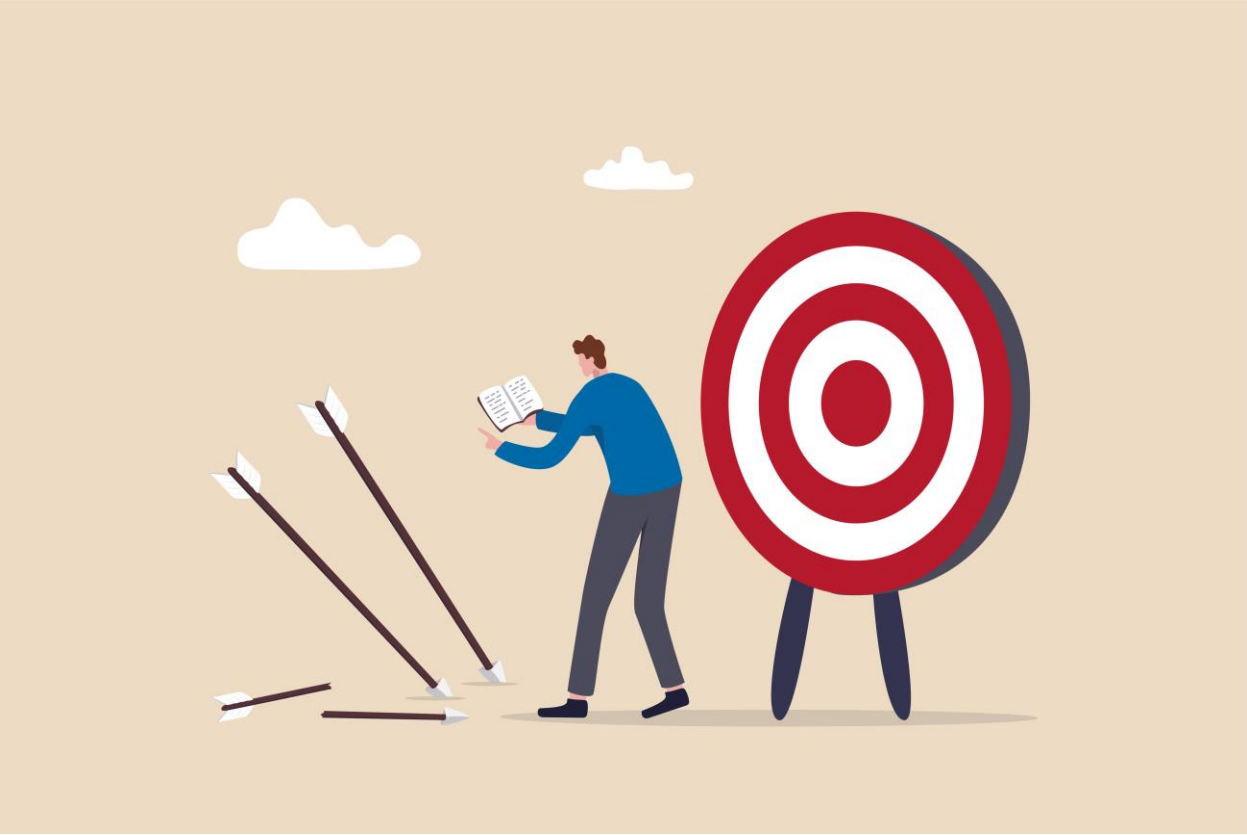
B2B Credit and Payment Fraud: Why You Should Be Prepared

No organization wants to be the target of fraud. Still, most see setting up and running effective fraud prevention as too imposing—more so than it is worth. As a result, organizations often leave fraud virtually unchecked, counting on the costs to remain low compared to prevention.

Fraud has an often unseen impact, however. Each case takes a toll on an operation's efficiency, a toll that gets compounded over the lifetime of the fraud scheme. The catch is that fraud typically goes on for far longer than organizations realize, and the cumulative impact is far more severe. It also tends to leave your organization and its customers open to information and identity theft.

Fortunately, fraud prevention is easier, and more achievable, than you would think. It requires a different set of risk tactics than most order-to-cash operations, as well as a knowledge of the fundamentals of B2B fraud. With those, however, organizations can build prevention strategies that work—and significantly under the costs, financially and operationally, of fraud itself.



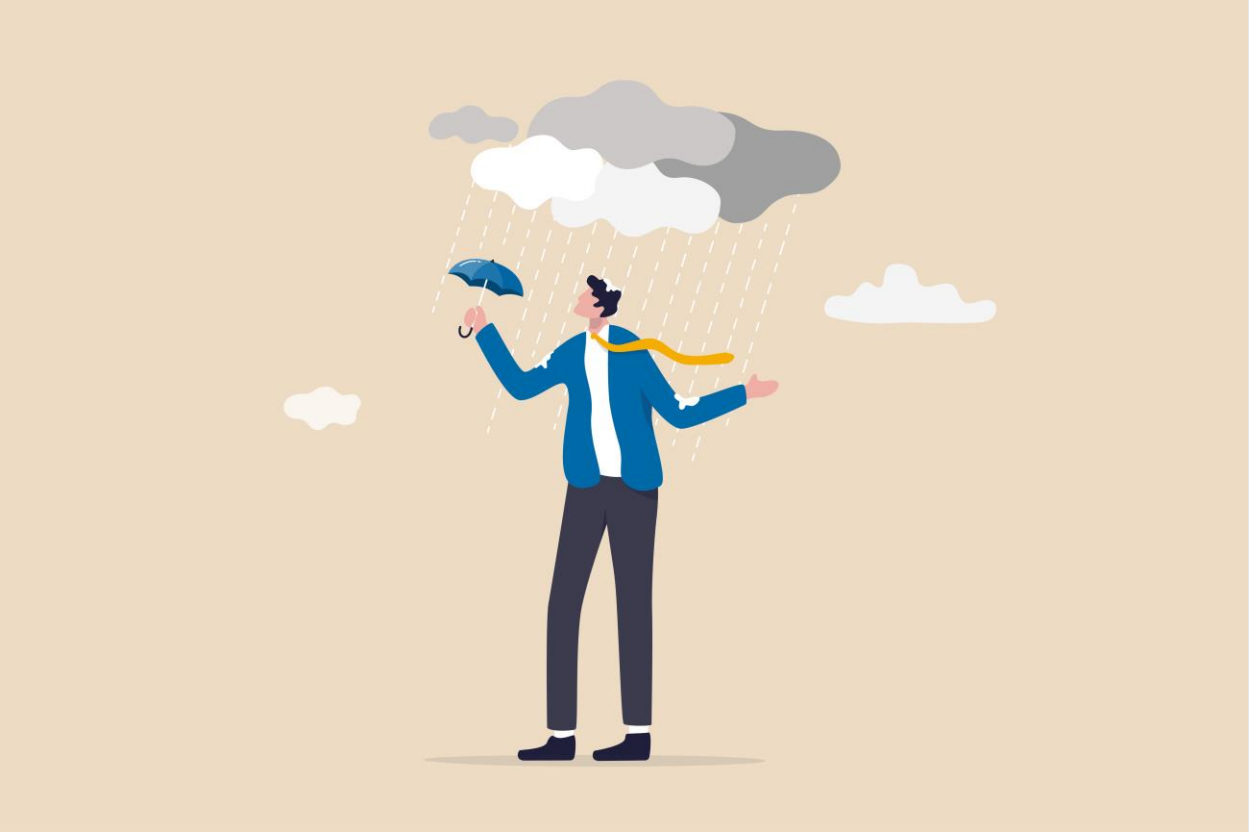
Why You Need to be On Top of Credit Fraud

Fraud's impact goes beyond revenue alone. To be sure, fraud's effect on profits is worth noting. The Association of Certified Fraud Examiners (ACFE), in its recent report, estimates that each year organizations lose five percent of their profits to fraud. More than that though, each instance

of fraud costs an organization time and resources, as operations continue to work accounts and transactions that, as frauds, will ultimately default. That burden compounds over a fraud case's lifetime—typically a full year according to the ACFE.

Add to that the fact that many forms of fraud also leave your organization vulnerable to information and identity theft. Company information and, even worse, customer information often become additional targets once scammers have found their way in.

Additionally, while the risk of fraud affecting your organization may seem distant, evidence shows that it is not. In its most recent report, the Association for Financial Professionals (AFP) reveals that 80% of organizations surveyed were targets of payment fraud in 2023.

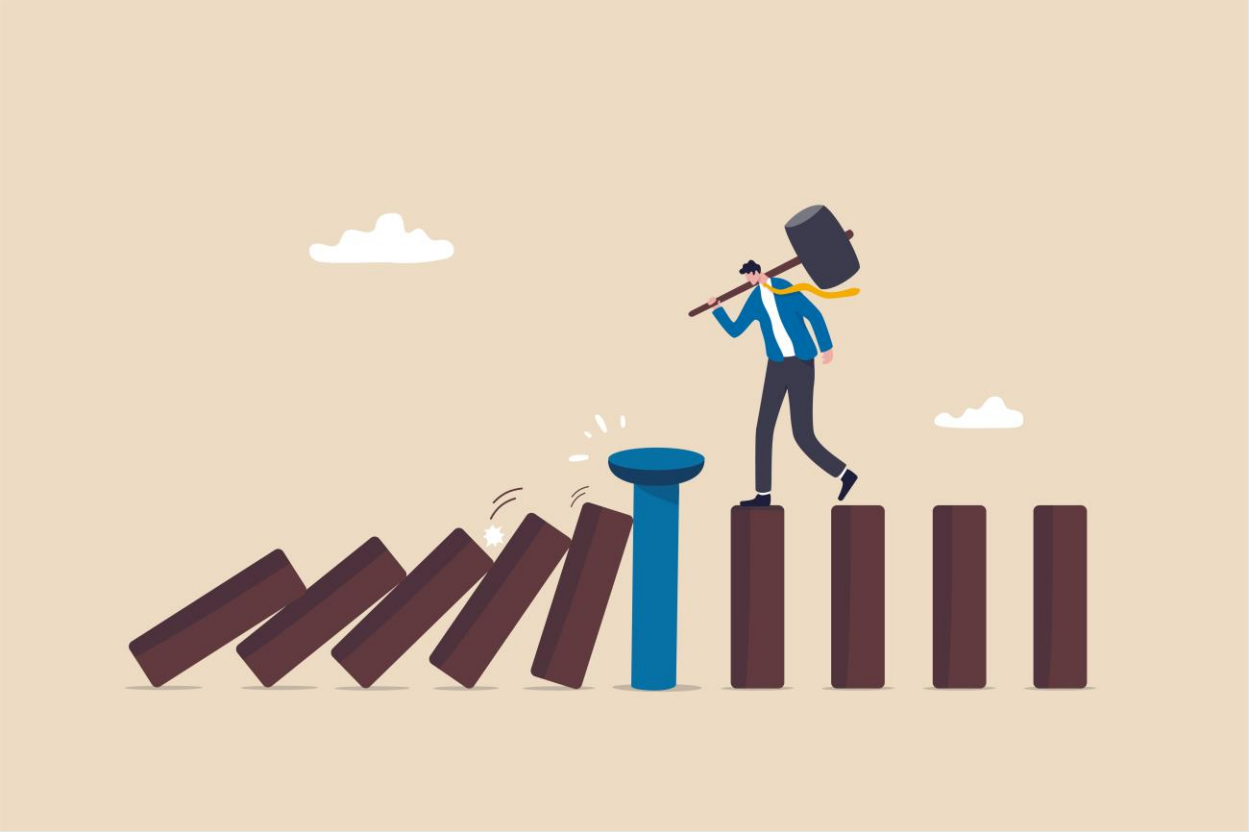


What You Can Do to Prevent Credit Fraud

The problem is that most organizations see fraud prevention as daunting—more so than the costs of fraud itself justify. However, that perception is largely due to the kinds of tactics these organizations deploy against fraud. Approaching fraud risk with the strategies of credit risk sets your organization up for massive inefficiencies—and without commensurate improvements in fraud prevention.

Fraud operates as a kind of arms race, with fraudsters and fraud preventers each upping the ante for the other, pushing them to new safeguards and exploitations. The result is a messy, difficult-to-predict, and constantly evolving field, one that traditional risk assessments cannot keep up with. Many organizations, seeing this, accept the consequences of fraud over the operational burden of prevention.

However, with the right tactics, fraud prevention is achievable, and far more easily and efficiently than you would think. The difficult and changing nature of the field means you need to understand the state of fraud and put together a comprehensive strategy designed for the unique challenges posed by fraud risk. Taking the right steps to do that, however, can secure you against fraud while keeping your operations smooth and efficient.



Know the Field

Credit and payment fraud can strike in incredibly diverse ways. Electronic fraud schemes proliferate with each technology. Discarded company hardware, compromised employee email accounts, similar domain names, and far more, offer fraudsters a world of options to choose from. Meanwhile, bad actors keep uncovering vulnerabilities for manual processes and paper forms. Schemes like falsified invoices and purchase orders—both on the rise—keep even that seemingly stable landscape unpredictable.

Yet despite the diverse methods, each instance of fraud ultimately comes down to either **impersonation** or **document forgery**. Additionally, to achieve those ends, fraudsters only have a relatively small range of information to work with. Regardless of the medium or trending tactics, fraud schemes all require stealing, manipulating, or fabricating one or more of these kinds of information.

- Bank account and funding
- Corporate status
- Personal and corporate identities
- Invoice/transaction history
- Asset status

It is important to be aware of particular fraud tactics, especially those affecting your industry. However, the strategy for safeguarding your organization against them centers on securing and verifying the information crucial to fraudsters' schemes.

Approach it Strategically

Fraud remains an unpredictable field, and to meet fraud effectively an organization's prevention strategy needs to be persistent and comprehensive. The challenge, even when you know the key information that fraudsters rely on, is keeping that information in continuous check without compromising your operation's efficiency.

Building your prevention strategy around the following set of core qualities, however, ensures your fraud coverage is complete and ongoing while also integrating prevention practices more smoothly into your order-to-cash operations.

- **Multi-layered.** Fraud may target any of the vulnerable kinds of information mentioned above. Ensure that each time you verify, you verify every applicable avenue of information. During account setup, for instance, verify individual and corporate identity as well as corporate status; for a transaction, verify bank funding and corporate status.
- **Immediate.** Fraud tends to be harder to deal with once it has started. Make verifications upfront as part of your account formation and transaction workflows. Catching fraud then spares your organization significant efficiency in the long term.
- **Informed.** Fraud relies on your organization only having a small—and inaccurate—picture. Verify information using the most up-to-date and authoritative sources. Holding definitive information makes your operation quicker and more accurate in identifying fraud.
- **Ongoing.** Fraud that lingers costs you more, and some fraudsters rely on waiting and creating a false sense of security. Monitor assets and corporate statuses continuously to ensure your organization can respond to fraud before it takes action.

These qualities follow two core fraud prevention priorities. While absolute fraud prevention is the ideal, the ACFE has found that the most effective prevention strategies adhere to these priorities to reduce fraud's organizational impact.

- **Rapid detection.** Cutting short the duration of any instance of fraud saves you order-to-cash efficiency—otherwise lost to ongoing fraud. In many cases, detecting fraud quickly can stop a scheme before it has done any damage.
- **Reduced losses.** Minimizing the cost of fraud prevents revenue losses—and also spares your organization significant risks for defaults. Some fraud schemes pivot on increasing costs, and strategies that reduce costs can keep these schemes from moving forward.

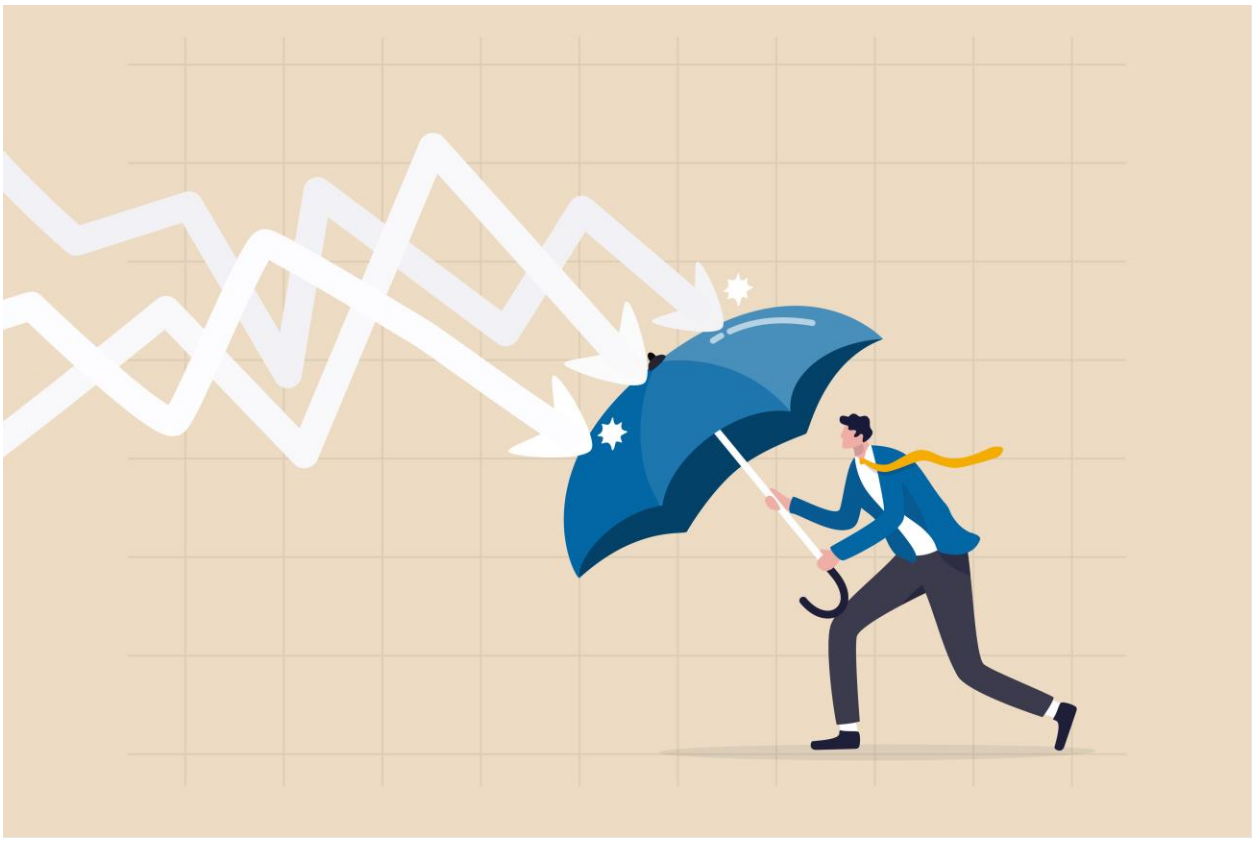
Multi-point Threats

Scammers may conduct multiple attacks, against multiple information types, at the same time. These "multi-point" attacks are prevalent in cases of disgruntled customers or customers in financial distress.

Such customers are motivated to exploit your business in particular. While individual strikes in these attacks may be small, they tend to be ongoing and destructive. In cases of disgruntled customers, you can expect attacks to extend to system compromise and information theft. Desperate customers, on the other hand, make wide-ranging attacks, starting small and escalating opportunistically more and more as time goes on.

The upside is that multi-point threats show patterns. These can be difficult to recognize at first but save you significant trouble and losses when you can catch them. Knowing how to distinguish customer distress is key, and our Credit Review Checklist provides a helpful guide.

Additionally, emerging AI solutions excel at pattern recognition. Machine learning algorithms can actively analyze credit and payment activities to discover patterns—and become proficient in spotting the unusual behaviors indicative of fraud. Dedicated AI services thus provide incomparably precise fraud prevention, all automatically and without interrupting transactions from good customers.



Adopting a Fraud-prepared Workflow

With a strategy following the tips above, an organization can begin implementing effective and efficient fraud prevention into their operations. The means of doing so are many, and the choices for each implementation will largely depend on operational needs.

That said, organizations will gain the most efficiency when their fraud prevention is integrated into their order-to-cash workflows and systems. In fact, the more seamlessly integrated the prevention is, the more efficiently it will run within your operations.

To that end, organizations have two key resources. The first taps your organization into dedicated fraud prevention tools, while the second makes those tools an effortless part of your organization's processes.

- **Use verification services.** Numerous services exist specializing in verification of different types of information—some verifying funding and bank account information, others corporate status, and others identity. These can streamline fraud strategy while simultaneously ensuring up-to-date and thorough verification.
- **Get platform integration.** Most order-to-cash platforms do not come with adequate fraud prevention out of the box. Platforms that support custom integrations can, however, potentially make verification services an automatic part your workflow. Doing so may

require a significant investment upfront, as well as routine maintenance, but even so the ultimate savings in efficiency and gains in fraud prevention can be dramatic. Each verification can take place automatically, at the point of transaction, as an effortless part of your operations.

The Platform with a Comprehensive Fraud Suite, Built in

Implementing a fraud prevention strategy is much like setting up anti-virus software. Some systems are vulnerable, and you would do well to get the best protection software. That takes effort to set up, the software may have a slight drain on performance, and you need to keep it up-to-date. Yet these compromises are worthwhile to keep a secure system.

Still, some other systems are built resistant, with security in mind from the ground up. These do not require you to set up and maintain separate protection software. Instead, the system itself manages everything, so you can do your best work, without ever having to think of prevention. Best of all, these systems tend to do prevention better, and without any performance impact.

One order-to-cash platform includes full fraud prevention similarly built into its fundamentals. Have your back covered with AI-assisted prevention, and get comprehensive verifications automatically with every transaction—all running seamlessly alongside your operations.

Learn more about securing your order-to-cash operations