

FRAUD PREPAREDNESS CHECKLIST



Fraud threatens more than your bottom line. It siphons productivity and puts your company's and customers' information at risk.

With this checklist, you can ensure your approach to prevention is effective. Whatever your industry—construction, food distribution, manufacturing, or otherwise—you can apply this checklist to safeguard your order-to-cash process. Doing so will help you do better business and foster better customer experience.

Checklist

Set Prevention Goals

Eliminating fraud is the ideal, but the priorities you set to achieve that can help you reduce the impact of fraud.

- ✔ Put rapid detection at the forefront of your planning to ensure fraud is less likely to happen and less likely to linger if it does happen.
- ✔ Aim to reduce the costs of each fraud occurrence, ensuring that you limit the damage done by any fraud that slips through.

Know the Risk Points

Be aware of the kinds of vulnerable information. Doing so helps keep you better guarded and prepared to prevent fraud.

- ✔ Bank account and funding
- ✔ Corporate status
- ✔ Individual and corporate identity
- ✔ Asset status
- ✔ Digital information



Understand the broad categories of fraud. These are the ways scammers manipulate vulnerable information to steal funds or data:

Impersonation. A scammer pretends to be a good customer, or pretends to be part of a trusted organization.

Forgery. A fraudster fakes legitimate documentation, or manipulates information on good documentation, such as references or invoices.

Digital misdirection. A con artist presents digital information that seems legitimate, with the goal of impersonating or forging. For example: using the email domain "@trustedcompany.com" to look like the real "@trustedcompany.com."

Keep up with rising fraud tactics in your industry. Watch for common tactics, but be alert to tricky new and novel ones as well. For example:

- ✔ Bust-out schemes
- ✔ ACH ghost funding
- ✔ Chargebacks on manipulated receipts
- ✔ Generative AI threats



Plan the Implementation

Know the leading verification sources.

Among these are:

- ✔ ACH verifications for bank account and funding
- ✔ Secretary of State databases for corporate status checks
- ✔ DMV databases for verifying personal identity
- ✔ Accurate lien filing and tracking to prevent asset fraud

Design fraud prevention strategically into your operations' workflow.

- ✔ Plan verification steps for each kind of vulnerable information.
- ✔ Determine when in your operations each verification should run.
- ✔ Connect with dedicated services for quick and accurate verifications.
- ✔ Incorporate verifications into your operations through operational training and system integrations.

Prepare methods and practices for continuous monitoring, ensuring that fraud has not occurred and is not ongoing.

- ✔ Assign responsibilities across the department to ensure accountability.
- ✔ Increase due diligence for high-risk accounts, and monitor their activity more closely.
- ✔ Periodically (e.g., monthly) audit customer information for to ensure it remains accurate and up-to-date.



Train Operations

- 1 **Disseminate** your fraud prevention strategy throughout the team.
- 2 **Ensure** each individual understands fraud vulnerabilities and responsibilities at their point in operations.
- 3 **Keep** the team up-to-date with your verification methods and services.
- 4 **Promote** fraud prevention as effective risk management.

Verifying Information

Independent verification is crucial for effective fraud prevention. Checking up-to-date and authoritative sources for vulnerable information is often all you need to keep a scammer from getting in.

The following are some of the top sources and services you can use to verify information.

- ✔ **Funding Source.** Use an ACH verification service. The service needs to verify both the funding amount and whether the funds have been resolved.
- ✔ **Corporate Status.** Check the Secretary of State databases. These will inform you of any bankruptcies and other corporate instability.
- ✔ **Personal Identity.** Look for the individual in Department of Motor Vehicles databases. These can verify whether an individual is who they claim to be and catch forged documents.
- ✔ **Corporate Identity.** Refer to reports provided by services such as Dun & Bradstreet's or Equifax's. Such reports can corroborate individuals with corporations.
- ✔ **Lien Status.** Complete UCC lien filings, which assures your rights. Add to this a service with lien tracking that ensures accurate and timely handling of the lien.
- ✔ **Digital Footprint.** Use a digital fraud detection service, which provides advanced fraud prediction on electronic transactions. An effective service can, for instance, match IP address and location to known corporate offices.

To-do

Information Checking	Identifying documents correct and current Individual's corporate association verified Corporate status current and in good standing Funding source verified Sufficient funding present and settled Assets not under existing liens All information independently verified
-----------------------------	---

Too many schemes exist to cover reasonably. This list prepares you against common and threatening schemes, and more broadly illustrates how to start assessing transactions in terms of fraud preparedness. Combine it with your own efforts to keep up with current fraud trends.



Checkpoints for Specific Schemes	Email address domain independently verified Invoices and/or receipts corroborated Digital details such as geo-location match the corporation Individual's employment is current and sufficient for the request Corporation has a sufficient credit history for the request
---	--

Learn about how all of this can be handled automatically for you, as an effortless part of a comprehensive order-to-cash platform.

Protect Your Business: Act Now to Prevent Fraud

[Click Here](#)

