PaymentWorks

Five Ways Your Vendor Master is Losing You Money: Mistakes and Fraud Edition

info@PaymentWorks.com

Follow us on in and 🐦

Mistakes are going to happen in any business, there really isn't any way around that. While it would be wonderful to eliminate the scourge of mistakes completely, that just isn't realistic. The goal, instead, should be to minimize exposure to risks while decreasing the high costs that come with onboarding and maintaining your vendor file. And make no mistake, the costs are indeed high. Benchmarking among our customer base indicates it costs $100-200 to onboard and maintain each of your vendors, each and every year you keep them as an active vendor in your file!

We have five ways your vendor file is losing your organization money, along with some practical advice on how to avoid these sneaky, unseen and often unmeasured costs.

1 Employees outside of AP collect vendor payment information

You would never ask a goalie to take a penalty shot, a fireman to perform heart surgery or a lawyer to change the alternator on your car. It's just not their job. So why are you asking somebody who isn't in procurement or accounts payable to collect TINs, remit addresses, banking info and W-9s?

Expecting employees who aren't familiar with collecting and vetting the credentials associated with vendor onboarding to do this type of work positions them as a 'go-between' the vendor and your AP department. This game of high-stakes telephone is not good business. It not only opens your organization up to the mistakes that come with the other four items on this list, it wastes tons and tons of valuable time for people on both ends of the transaction.

While you may want your larger organization end users to have the say in who they do business with, having a central point tasked with collecting vendor documents will eliminate many potential entry points for fraud vectors and reduce many of the hidden costs that go into the $100-200 you pay per year to onboard and maintain each vendor.

HOW THIS COSTS YOU:

- increases opportunity for fraud
- increases time spent onboarding vendors
- department employees spending time on functions not integral to their jobs (our benchmark is 37 minutes per vendor that the business owner spends on each new addition)

2 Manual mistakes (aka the 'fatfinger')

The human element of mistakes runs the gamut from typos to using an old remit address to attributing a piece of information to the wrong company. It's also, shockingly often, just sloppy handwriting — ask anyone who has ever had to decipher a handwritten W-9.

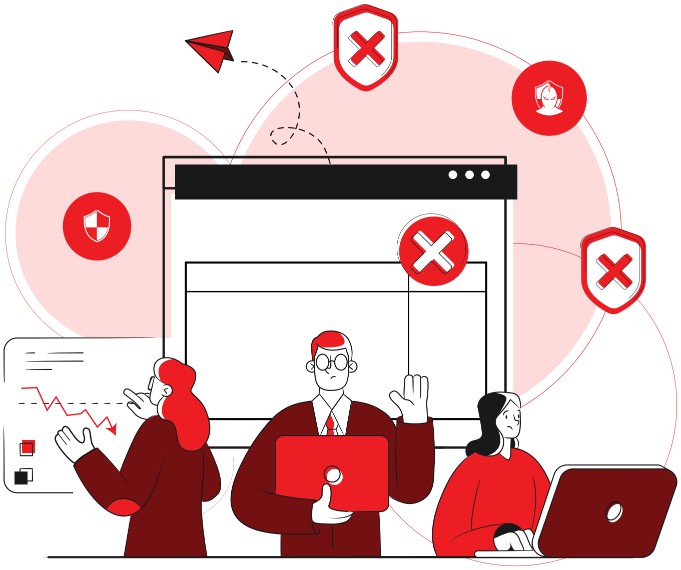
If you are leaving things to chance by asking your AP staff to collect and input information manually from paper forms into the ERP, then it is practically a guarantee that your data is not clean.

Additionally, many, many organizations continually struggle with what we call 'the dilemma of duplicates,' aka, dupes in the vendor file. New order addresses often end up creating new vendor records, which in turn creates a mess.

HOW THIS COSTS YOU:

- returned checks for incorrect addresses
- charges for returned ACH for incorrect routing or account numbers
- time and effort finding, correcting, and reissuing payments
- B Notice Violations from the IRS for incorrect 1099s
- time wasted on duplicate vendor entries, then subsequent time untangling the inputs

3 Accepting unconfirmed vendor information into your ERP



If you already have a main point that collects all of this vendor info, you have already eliminated a lot of these hidden costs for your org. The next question to ask is if you are leaving it up to an employee to use their own judgment to determine if what they have collected is legit? And if changes related to what is already in your ERP (a name change or a banking change request) are legit? If so, the door is open for risk exposure and a lot of potential costs.

Without tools to vet and confirm, your staff are left to sift through reams and reams of information, attempting to spot mistakes and fraud with nothing more than their eyeballs.

When your staff is armed with tools to confirm the vendor credentials, they are relieved of the significant stress of attempting to ascertain what is true and what is a scam. By using third parties to confirm credentials like TIN, address and banking, your organization will have much greater peace of mind.

HOW THIS COSTS YOU:

- see #2
- especially see #4

4 Bad actors and social engineering

This one is the big fear: payments fraud. Social engineering is the easiest way for a fraudster to steal your cash. It doesn't even require the savvy of a computer hack (though it often starts that way). Social engineering is essentially when one party uses email or the phone to trick another party into doing something they believe is legitimate — usually involving transferring large sums of money into a fraudster's bank account. These types of fraudulent scams can happen on scales large and small-you probably read about them every day.

If your current process allows for payment details to be changed because your AP staff received an email with new banking instructions, or even after they talk to someone on the phone then please put this risk at the top of your list of ways your vendor mafilester is costing you, because sooner or later, someone is going to get fooled.

HOW THIS COSTS YOU:

- paying a fraudster instead of your vendor
- potential litigation with your insurance company to cover the money you lost
- risk exposure benchmark at .059% of your annual spend: this is what your potential fraud loss is each year
- reputational loss
- job loss (this is the mistake that gets people fired)

> Phone calls are no longer a completely reliable means of vetting bank account details. If you reach the vendor with an outbound call to a verified phone number, you are good. If you leave a voice mail, and receive a return call from a number that you don't recognize, then you cannot be sure you are talking to the real vendor.

5 Storing bank accounts in your ERP

This might be a fraud vector that some people don't worry about too much. Because you trust your employees, right? Depending on who has access to your ERP, someone on the inside could change bank account details.

This risk alone would be enough of an argument to get out of the business of storing bank account numbers, but you're also vulnerable to bad actors on the outside being able to hack into your ERP and change an account number. So finding a partner or system that takes banking accounts out of your ERP could eliminate a huge fraud vector that you might not even be considering at the moment.

HOW THIS COSTS YOU:

- another opportunity for fraud - inside or outside
- Reputational harm

Taking necessary precautions to reduce fraud and human error is just smart business.
Audit these five areas now and preemptively put in roadblocks will save you time, money and allow your employees to mind your business, and stop worrying about threats.

info@PaymentWorks.com

Follow us on in and