Fight payments fraud by locking down your vendor master

How secure are your organisation's controls around onboarding new vendors and updating their details? ***Taylor Nemeth*** *of PaymentWorks provides pointers on a secure process.*

Goldmine

Right now, finance professionals are losing sleep over the threat of falling victim to a payments fraud scam. And the latest AFP Payments Fraud and Control Survey [1] reinforced that there is every reason to fret – an alarming 74 per cent of companies reported that they were the target of an attempted or actual payments fraud scam in 2020, while 30 per cent reported an *increase* in attempts over 2019.

The report highlighted that 76 per cent of these frauds or fraud attempts originated from a business or vendor email compromise, and a disturbing 34 per cent of victims didn't even notice a successful fraud for more than two weeks after it occurred. This is particularly disappointing – as the more time that passes before uncovering the event, the less likely it is that an organisation can recover the stolen funds. The main target of these attacks? In 61 per cent of the cases, it was the accounts payable staff.

To add to the list of ulcer-inducing news, the Federal Bureau of Investigation's Internet Crime Report also recently noted that business email compromise accounted for nearly US$2 billion in losses in 2020. [2]

These alarming numbers can evoke a feeling of inevitability: it is 'not if but when' your organisation will end up on the wrong end of these statistics. But while you cannot do anything about the attempts, falling victim to a payments fraud scam doesn't have to be a *fait accompli*.

Begin at the beginning

The breakthrough for a fraudster in a payments scam almost always starts by tricking someone on your staff into changing the bank account credentials for a vendor. If you want to fight the fraudster, you must begin with the vendor master. Moreover, you must begin where the vendor begins: when submitting identity credentials with the goal of getting paid.

There are myriad reasons why this entry point is an attractive target for a would-be scammer. Many large organisations, especially those in higher-education, healthcare, construction and state or local government, have distributed procurement. This means there are multiple people, in some cases upwards of 10,000, within the organisation who have the authority to choose who they want to do business with.

Locking down the vendor master starts with vastly narrowing who is responsible for actually onboarding the vendor. You can give your departments the autonomy to make their own business decisions; however, immediately remove them from the manual, paper-intensive process of onboarding vendors. This type of distributed onboarding is simply not compatible with upping your business controls to prevent fraud. Governing such controls across thousands of users is untenable and, as a result, risky. When you centralise the entry point for your vendors and make the collecting and vetting of vendor information someone's job, you can narrow the point that a fraudster can enter to just one.

While having one way in is ideal, you still need to guard that point of entry fiercely.

Trust, but verify

Once you have locked down the ownership of vendor onboarding, you need to consider how those owners will validate the collected identity elements and ensure they are true and accurate. The two most important elements to confirm when shoring up your defences against payments fraud are the tax identification number and bank account ownership. Let's start with the easy one: the tax ID.

Tax ID: What you need to know is simple – is the TIN a valid number? Does it belong to an individual or an entity? Does it belong to the payee you intend to pay? Beyond preventing fraud, ensuring accuracy will have a huge impact come tax time. There are a variety of third parties you can subscribe to that will validate the accuracy of the tax ID. If you aren't doing this yet, start today. Having a person at your company submit data to a third party can be time consuming, but the payoff in data accuracy is 100 per cent worth this effort. (Next level: technology partners that the payee submits information to themselves, saving your staff the effort).

And now for the not-so-easy: bank accounts.

Bank account ownership: Preventing a social engineering scam comes down to this – have you verified that the tax ID you have just confirmed is actually associated with the bank account you are paying? The effort your humans will have to put into this step, while possible, can easily take a full-time position to maintain. Phone calls to the payee, while simple and effective, are a challenge, particularly with a continued reliance on remote working. Getting someone to answer those calls is proving to be increasingly difficult and can take days, or more, to complete.

Speaking of phone numbers – are you calling a confirmed number? One you are certain belongs to the entity you intend to pay? You certainly cannot trust just any phone number delivered to you via email, so having a technology partner to validate the phone number is a key, and often overlooked, piece of your security puzzle.

There are ways to confirm bank account ownership via third parties, but many are limited in scope, capable of verifying only some accounts at certain banks or only focused on specific countries. When your staff are responsible for this step, your vendor onboarding process can come to a grinding halt. Finding a partner who can verify as many of these types of accounts as possible, in a reasonable amount of time, is critical to preventing the risk of business payments fraud. Every third-party validated account is one less account your staff need to confirm themselves.

When self-verifying bank accounts, consider these fraud vectors and red flags:

- Hacked emails provide phone numbers that dial straight to a fraudster – are you sure you are dialling the real company?
- Time of day for change requests: did the change arrive outside of the vendor's normal business hours, say at 4am on a Saturday?
- Can you pinpoint geolocation? Is the vendor located in Indiana, but the email requesting the change is originating from Latvia?
- Has someone at your own company been socially engineered to push for this change?
- Do your controls consider ways to vet internal requests that do not involve email?

The one constant: change

In our experience, 30 per cent of vendors will change at least one piece of their identity information at least once each year. We've heard time and time again: updating information in the ERP (enterprise resource planning software) is hard. So hard, that many (most?) organisations do not have an established process to support it. Do they have a separate form for vendor updates? Probably not. Do they go through a centralised process in AP/Procurement? Probably not. Do the departments and business units still deal with the vendor regarding this change? Probably!

Updates are time-consuming and challenging without a process, system or clear internal ownership of accepting and making the changes. All of the actions you have just taken (assigning ownership of onboarding new vendors, confirming tax IDs, confirming bank account ownership) you now need to apply to changes. In fact, this is arguably the most vulnerable piece of your vendor master management puzzle, and the one many fraudsters are likely to try to exploit – particularly when there is urgency around the timing of a payment.

The owners of your vendor master need to be charged with owning not just the onboarding and vetting of new payees, but also any changes submitted for vendors that your organisation is already working with. As with the new vendor information, vetting the changes can be very time-consuming without partners in place to verify the changes, particularly related to tax IDs and banking.

It is fair to say that fraudsters have noticed and exploited all that is involved with vendor onboarding and maintenance. Getting it right is important. Seventy-six per cent of you reading this will have an attempted fraud happen at your company this year. Thirty-four per cent won't catch a successful fraud in time to pull back any of the funds. This problem deserves your attention. If you don't have the means in-house to lock down your vendor master data, leverage an investment in key technology partners who will do the heavy lifting and guarantee their work; you will gain security, peace of mind, as well as ensure a good night's sleep!

Notes

1. www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud
2. www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Taylor Nemeth is head of payments at PaymentWorks (www.paymentworks.com) where he is responsible for the strategy, operations and growth of the company's Payment Security solution. He previously managed payments products in the higher education sector for CBORD.

May 25 2021