

At PaymentWorks, we know AP and Procurement professionals lose sleep worried about fraud and compliance risk with their vendor master file. Use these 10 questions to assess. **Is your current vendor onboarding and maintenance process locked down, efficient and compliant?**

1	Have we ever <b>paid a fraudster</b> instead of our intended payee? Have there been close calls?
2	<u>Are we relying on easily forged items</u> such as voided checks or banking letterhead as proof of bank account ownership?
3	Does our payee onboarding procedure have an <b>audit trail</b> ?
4	Do we check <b>sanctions lists</b> with every PO issued, or just at the time of initial vendor onboarding?
5	Do we know the internal costs incurred for <b>manual efforts</b> around payee onboarding?
6	<u>Are employees across our organization</u> charged with <b>collecting sensitive identity elements</b> such as TIN and banking information from payees they want to onboard?
7	Are we handling <b>paying individuals and complex business entities with the same process</b> ?
8	Does your vendor desk team know that <b>NO ONE in your organization would ever ask them to break the onboarding or updating process</b> 'just this one time'?
9	Do we accept incoming calls from vendors at <b>unverified phones numbers</b> (e.g., cell phones) to <b>confirm banking information</b> ?
10	Does our <u>cyber insurance policy cover losses</u> due to <b>an employee being tricked</b> i.e., when there is no actual breach involved?

**If your answers to any of these questions make you think your process may be vulnerable, inefficient, or worse, then find out how to address these warning signs at [PaymentWorks-See How it Works](#) or [request a demo](#) today.**