PaymentWorks

Preventing Payments Fraud: Assessment Questionaire

Examining your payments process with a focus on finding and closing all of the holes a fraudster could potentially exploit is daunting. We get it. To guide your effort, we've created this quick assessment focusing on five areas you should examine:

1 New vendor onboarding and approval

2 Re-examine your existing controls

3 Have an audit trail

4 Verify all identity elements before accepting them into the ERP

5 Insure against losses

1 New vendor onboarding and approval

□ Do people at your organization have free rein to determine who they want to do business with?

□ Do you have controls in place to limit the number of vendors you do business with in a particular category, for example: how many different office supply vendors do you use?

□ Do you have controls in place regarding inviting or approving new vendors?

□ Can business be initiated prior to an approval and onboarding of the vendor?

□ Is your process followed?

2 Re-examine your existing controls

□ Who specifically, or which department, owns the vendor onboarding process?

□ Are the owners responsible for gathering the required sensitive vendor identity credentials such as W9, Tax IDs, and insurance documents, or does that fall to departments?

□ Are those responsible trained to spot obvious fraud attempts, fakes and forgeries?

□ Are those responsible trained in detecting social engineering attempts?

□ Do you have controls in place regarding who has access to vendor identity details?

□ Do you have controls in place regarding who has access to changing vendor identity details?

□ Do you have controls in place for the "minimal acceptable standard" you will accept before changing existing vendor identity elements?

□ Are you using 3rd party partners to verify the authenticity of the submitted credentials?

3 Have an audit trail

- ☐ Can you clearly chart the vendor onboarding process, including who invited and who approved the new vendor?
- ☐ If approvals are needed from myriad departments (conflict of interest from HR, sanctions alerts from compliance, insurance documentation from risk), are the approvals time stamped, collected and stored in a centralized location?
- ☐ Are you collecting and storing the required vendor documentation, such as proof of insurance, with expiration date notifications in place?

4 Verify all identity elements before accepting them into the erp

- ☐ Are you verifying tax IDs?
- ☐ Do you confirm bank account ownership and validity before making a payment?
- ☐ Do you regularly monitor sanctions lists to ensure you are not doing business with companies on these lists?

5 Insure against losses

- ☐ Does your risk, cybersecurity or crime insurance policy cover monitary losses due to email compromise?
- ☐ Does your risk, cybersecurity or crime insurance policy cover monitary losses due to human error?
- ☐ Do you have a reserve fund set aside in case of a payments fraud that will cover anticipated losses so you do not need to cut critical budget items elsewhere?

We can help. PaymentWorks automates complex payee-management processes for every payee to eliminate the risk of business payments fraud, reduce cost and ensure regulatory compliance.

Request a demo at: info@paymentworks.com

Follow us on in and 🐦