Account Payable Fraud

The increasingly sophisticated tactics that criminals employ make it harder for businesses to identify fraud. And fraud is indeed on the rise. Social engineering scams, which trick employees into sending money or providing sensitive information, accounted for 50% of fraud incidents among small and medium-sized enterprises (SMEs) between January and August of 2022, according to "The Overlooked Importance of Securing Incoming Payments," a recent report from PYMNTS and nsknox. **Invoice fraud has also accrued an annual average of $280K in losses per SME company in the last year.**

Nonetheless, many businesses are not allocating sufficient funding for fraud prevention, particularly within their accounts receivable (AR) operations. It is critical for SMEs to educate themselves about the risks of the lack of fraud prevention efforts.

On the Radar Now

Despite the prevalence of fraud related to accounts payable (AP), it is a largely underfunded area within many organizations. Meanwhile, the COVID-19 pandemic, the increase in online activity, and the proliferation of remote work pushed many businesses to embrace digital AR/AP platforms.

According to PYMNTS' findings, 56% of retailers have purchased AR platforms since the onset of the pandemic, while 64% of companies that have yet to do so are in the process of implementing or gearing up to add them. At the same time, though few companies publicly discuss the issue, internal AR fraud **accounts for roughly $1.8MM in average losses within organizations.**

At present, only 38% of organizations employ fraud prevention tools specific to AR, such as identity and document identification, which leaves businesses vulnerable to fraud both in the areas of AP and AR.

Increased Awareness

Though AP and AR fraud prevention aren't at the top of some SMEs' lists when making budgets, there are signs that this may change. A growing number of chief financial officers (CFOs) are beginning to invest more actively in digital risk management and fraud prevention measures. PYMNTS found that 85% of CFOs have either begun investing in digital fraud prevention solutions or are planning to do so.

One reason this is necessary is that, even though AP and AR fraud have been on the rise, fraudsters are often successful in their efforts to siphon funds because an overwhelming number of businesses fail to authenticate identities or account information if it appears

legitimate. The Better Business Bureau recently sent out a scam alert to bring awareness to a rise in invoice scams, where the invoices claim to come from PayPal or Best Buy subscription services or purchases, and small businesses have fallen prey to these fake invoices.

Preventative Steps

Small and medium-sized enterprises can reduce potential fraud by investing in fraud prevention measures and becoming educated on the most common tactics of fraudsters, such as the aforementioned invoice scams and hacking into email servers. Once fraudsters gain access to a company's servers, they are able to easily fool customers into paying what appear to be legitimate invoices, but the payments are actually routed outside the company.

With B2B payments projected to increase at a 6% compounded annual rate between 2022 and 2030, such fraudulent activity is expected to continue rising. Combatting this type of fraud requires that SMEs ensure they have strong internal controls in place, such as:

- Mandating that email is never the sole way payment requests are handled.
- Ensuring interactions with customers are made solely through secured channels, like encrypted email inboxes.
- The identity of an individual requesting payment and any information they provide is always authenticated.

Online fraud isn't going away. As it becomes more sophisticated, it is extremely important that businesses focus their security efforts on the appropriate areas.