5 ways to reduce mining and construction payment fraud in SA

In 2021 there were 230 million cyber threats detected in South Africa, by far the most activity on the continent. As one of the top 10 mining countries in the world, South Africa's economy relies heavily on this industry as well as those closely related to it, such as construction. These conditions also make it a prime target for bad actors.

Ryan Mer, CEO eftsure Africa. Source: Supplied

The mining industry is among the most at-risk industries for fraud and in some countries it tops the list of revenue lost due to fraud, closely followed by construction. Due to the nature of these industries and the often-elaborate fraud schemes that target them, huge losses can result from just one instance of fraud.

Furthermore, fraud is on the increase - PwC's Global Economic Crime and Fraud Survey 2022 revealed that 51% of organisations have experienced fraud, corruption, or other economic crimes in the last 24 months.

"Clearly, today's CFO needs to be highly attuned to the constantly evolving fraud landscape," says Ryan Mer, CEO of eftsure Africa, a know your payee (KYP) platform provider.

"Payment fraud, supplier fraud and tender-related fraud poses a significant risk in the mining and construction sectors in South Africa. Companies operating in these industries need to stay on top of ever-evolving fraud trends and adapt their defenses accordingly, or it could impact their financial stability." Mer gives these tips to do exactly that:

1. Never neglect background checks

Mining and construction companies require comprehensive background checks to verify the credibility of suppliers. In addition, South Africa's Mining Charter, which sets out to achieve inclusive procurement, and supplier and enterprise development, requires organisations to record and report on these as part of general due diligence and compliance.

These background checks should involve scrutinising supplier directors, checking for any politically exposed persons (PEPs) and sanctions, and linking directors to employees.

Companies with international suppliers may face limitations in verifying foreign supplier information, adding complexity to fraud prevention efforts. Nevertheless, these companies can still utilise onboarding platforms and automated verification processes for local suppliers to enhance efficiency and reduce payment fraud risks.

Not only will these extensive checks ensure compliance, but also help identify potential risks and reduce the likelihood of fraudulent activities.

2. Collaborate to reduce costs

Mining and construction businesses can consider partnering with specialised companies to conduct background checks on suppliers. Such companies offer extensive reports that include crucial information for assessing supplier credibility.

Nersa agrees with decision to procure electricity from SADC region

31 Jul 2023

The challenge lies in determining the pricing structure for these reports, as they typically charge per report. Balancing the costs of these verification reports while maintaining competitive pricing structures will be crucial for success. Consider negotiating collaborative contracts with these companies or integrate the price into services offered to offset costs.

Once an organisation has credible background reports on its suppliers and vendors, it's crucial that continuous payment control and monitoring measures are in place to protect the integrity of key supplier information, including payment details.

3. Keep training up to date

As threat protection becomes more sophisticated, fraudsters are targeting people to circumvent digital security measures. Digital security really does help, but personnel training is crucial. Otherwise, it's like having the best security at your house, from beams to alarms to fencing, and letting someone through the gate without checking their credentials.

And don't stop there: training materials must be regularly updated as fraud trends change, and employees must be made aware of these updates.

4. Don't just automate, integrate

Because people are often the weakest link in the security chain, most companies today have automated processes in place to minimise the risks associated with manual processes. The next step is to not only automate, but to integrate.

A Software as a Service (SaaS) provider can help enhance processes and limit payment fraud risks by providing an integrated onboarding, verified master data management and payment screening solution that cross-references the payments an organisation is about to release with a database of verified bank account details.

This can be integrated into anything from ERP and accounting systems to sales and customer relationship management systems. The platform alerts you to any potentially compromised payment details, allowing you to deal with the problem before the flow of funds has occurred.

5. Insure, in case

Even with the best mechanisms in place, it's still possible to become a victim of fraud. Fidelity insurance is a class of insurance designed to protect against losses resulting from fraud or theft by an employee and is crucial to the survival of one's business in such instances.

One of the main requirements of a fidelity policy is to have mechanisms for checking and controlling accounting and business processes.

"Having the above measures in place will not only help prevent any losses from occurring in the first place, but will also decrease spend on fidelity insurance premiums and ensure that any losses that slip through the cracks will be covered," concludes Mer.