

August 22, 2023

Invoice fraud alert! Don't get caught with your pants down



Louis J. Freeh wrote, “*The fraudster’s greatest liability is the certainty that the fraud is too clever to be detected*”.

Invoice fraud has become a reality we cannot deny, and something which we should be educated on and face head-on.

Invoice fraud is essentially a fake payment request sent by fraudsters, acting as your regular and trusted supplier.

The intention behind these masterful fraudulent activities is to extract a sum of money from a company – undetected, untraceable and undeniably sly.

What are the types of invoice fraud?

- Inflated invoices
- Fraudulent invoices
- Compromised email threats
- Internal fraud
- Duplicate payments
- Non-delivery of products or services

How is invoice fraud done?

This is a complex crime and starts long before the fake invoice or falsified email is sent.

Fraudsters infiltrate your company's database or email thread which contains private and payment information – they then target the accounts payable process and exploit weaknesses in a company. An illustrative instance involves businesses utilising external payroll service providers. Fraudsters craft emails mirroring the company's information, which are then dispatched to the service provider, containing modifications to employees' banking particulars. Acting under the assumption that these directives originate from their customer, the service provider enacts these alterations. Consequently, when the payroll process is completed, funds are disbursed to inaccurate accounts.

The rise of e-commerce has also given rise to fake company websites and social media accounts designed to deceive customers into divulging sensitive information or making purchases that never arrive. Fraudsters replicate legitimate websites, complete with convincing layouts and branding, to lure unsuspecting consumers.

Tips to prevent invoice fraud

- o Establish a good customer relationship with your supplier/client and regularly make contact – increase trust levels.
- o Regularly change passwords and update cyber security to avoid unusual sender requests.
- o Keep an eye on supplier activity – a sudden change in a supplier’s usual process or sudden strange links in their emails may be an indication that something is not right.
- o Stay on top of changes in payment information – a sudden change in banking details or being pressured to pay out of the blue should alert you.
- o Match invoices and quotations to detect discrepancies.
- o Educate employees about the risks of fraud and monitor related strange and erratic employee behaviour.
- o Avoid sharing personal information or making purchases on unfamiliar sites.
- o Check the website's URL, look for security indicators like HTTPS, and read reviews.

In conclusion

As a leader in *business legal compliance solutions*, we see attempted scams more than we would like to. Anyone can fall victim to this increasingly prevalent crime; therefore, you and your staff should always be one step ahead of those who consider themselves Masterminds. The fight against fraud begins with awareness, prevention, and vigilance.

Access to information and the protection of certain types of personal information rights in South Africa are entrenched in the Constitution and are mainly regulated by the *Promotion of Access to Information Act (PAIA) and the Protection of Personal Information Act (POPI)*.

Cybersecurity software and education can go a long way in preventing falling victim to these scams. It's essential for individuals and organizations alike to stay informed about evolving fraudulent tactics.

At SERR Synergy we provide corporate legal solutions, including *protection of personal information to better assist you in safeguarding your data and staying one step ahead of the fraudsters.*

About the Author: Deseree-Lee van der Watt holds a LLB degree from the University of Pretoria. She proudly manages our BEE departments in both the Free State and Northern Cape.