Lync Wealth Management

A Guide to Protecting your Business

Tel: 01565 658 840

enquiries@lyncwealth.co.uk

www.lyncwealth.co.uk

Introduction

In today's fast-paced digital landscape, where technology advancements have opened new avenues for business growth, they've also brought about an increased risk of fraud. As a financial business owner, ensuring the safety and security of your operations is paramount.

With over £1.2bn stolen through fraud in the UK in 2022, whether you're a seasoned business owner or just starting out, safeguarding your business from fraud is an ongoing concern. From cyberattacks to insider threats, this resource will equip you with an understanding of some of the various forms of fraud that can target your business. We'll delve into practical strategies, advanced technologies, and expert insights that arm you against these threats.

What is business fraud and where can it come from?

Business fraud is defined as “the intent or the act of misrepresentation”. This means scammers lying about themselves or their actions and services to cause gain or loss.

Fraud can come from a variety of means, more often than not it comes from employees, ex-employees and suppliers but unfortunately the reality is, it can come from absolutely anywhere, even people not connected to your business in any way.

The monetary loss from fraud can be crippling and cases can take a long time to prosecute because they are often complex.

Different types of Business Fraud and how you can prevent them

Employee theft

One of the most common forms of business fraud is employee theft. Employee theft, also known as employee fraud, refers to the unauthorised taking or misuse of an employer's assets, funds, or resources by an employee. It involves dishonest actions by employees who exploit their positions within the organisation to gain personal benefits at the expense of their employer. Employee theft can take various forms, including:

Misuse of Company Resources: Employees use company property, equipment, or resources for personal purposes without authorisation, causing financial losses to the organisation.

False Expense Claims: Employees submit fake or inflated expense reports to receive reimbursement for expenses that were never incurred or were personal in nature.

Inventory Theft: Employees steal goods, products, or inventory from the workplace for personal use or to sell elsewhere.

Skimming: Employees divert cash from sales transactions before it is recorded in the company's accounting system.

Billing Schemes: Employees create fake invoices or alter billing records to channel payments to their personal accounts.

Payroll Fraud: Employees manipulate payroll records to receive unauthorised salary increases, overtime payments or benefits.

Data Theft: Employees steal sensitive company data, customer information or intellectual property for personal gain or to sell to competitors.

Procurement Fraud: Employees manipulate the procurement process to overpay suppliers or receive kickbacks for awarding contracts to specific vendors.

Employee theft can have significant financial and reputational consequences for businesses, affecting profitability, employee morale, and customer trust.

Employee Theft Prevention

Preventing employee theft requires a combination of proactive measures and a strong culture of integrity within the organisation. Here are some strategies that can help to prevent employee theft:

Background Checks: Conduct thorough background checks on potential employees before hiring them. This can help you to identify any criminal history or other red flags that could indicate a risk of theft. This includes gaining at least 2 references, at least one being from the most recent employer. Unless the individual can provide valid evidence of why they cannot provide a reference from their most recent employer, this can be seen as a red flag as they could be hiding the real reason why they are seeking new employment.

Policies and Procedures: Develop and implement clear policies and procedures for handling cash, inventory, and other valuable assets. Make sure employees understand these policies and are trained on how to follow them.

Access Control: Limit access to areas of the business where valuable assets are stored or handled. Managing keys, passwords, or other access control measures will ensure that only authorised employees can access these areas.

Regular Audits: Conduct regular audits of your inventory and financial records to detect any discrepancies or anomalies that could indicate theft.

Reporting Mechanisms: Establish a reporting mechanism that allows employees to report suspicious behaviour or activities without fear of retaliation. In most cases, this will mean encouraging employees to report to their line manager. Eventually, the report will need to be made to the relevant authorities.

Employee Education: Educate employees on the consequences of theft, both for the company and for themselves. Make it clear that theft will not be tolerated and that there will be consequences for any employee who engages in it.

Invoice Fraud

Invoice fraud, also known as invoice manipulation or false invoicing, is a type of financial fraud where individuals or entities intentionally create or alter invoices with the aim of deceiving a business or individual into making unauthorised payments. It often involves tricking the victim into paying for goods or services that were never delivered, overcharging for legitimate goods or services or diverting payments to fraudulent accounts. Invoice fraud can take various forms, including:

Fake Invoices: Fraudsters create entirely fake invoices for goods or services that were never provided. These invoices may appear legitimate, complete with false details and contact information.

Altered Invoices: Fraudsters modify genuine invoices, changing the payment details such as bank account numbers to redirect payments to their accounts.

Overcharging: In this scheme, legitimate invoices are inflated with higher prices than agreed upon. The victim pays more than what was originally agreed for the goods or services.

Double Invoicing: Fraudsters send multiple invoices for the same goods or services, hoping that one of them will be processed without proper scrutiny.

Phishing: Fraudsters impersonate a legitimate supplier via email or other means, sending invoices with altered payment instructions. Unsuspecting victims then make payments to fraudulent accounts.

Ghost Employees or Suppliers: Fraudsters create fake employee or supplier profiles and generate invoices for services that were never rendered or goods that were never supplied.

VAT or Tax Fraud: Fraudsters manipulate invoices to evade taxes by charging less than the required tax amount or not reporting taxes at all. Invoice fraud can result in financial losses, damage to business relationships, and reputational harm.

Invoice Fraud Prevention

Businesses and individuals can take several steps to mitigate the risks of falling victim to invoice fraud:

Verify Invoices: Always verify the legitimacy of an invoice before making a payment. Check that the invoice matches the agreed-upon price, and that the supplier is a legitimate business.

Verify Suppliers: Verify the identity and legitimacy of your suppliers before doing business with them. Check their contact information and company details and use reliable sources to confirm their identity.

Use Purchase Orders: Use purchase orders to set out the details of each transaction, including the goods or services ordered, the agreed-upon price, and the delivery date. This can help to prevent unauthorised purchases and ensure that invoices are legitimate.

Implement Internal Controls: Implement strong internal controls, including separation of duties, to prevent unauthorised access to financial systems and reduce the risk of fraud.

Educate Employees: Educate employees on the risks of invoice fraud and how to recognise and report suspicious activity. This can include training on phishing scams, fake invoices, and other common fraud tactics.

Employee Training: Educate employees about invoice fraud, phishing, and other fraudulent schemes, emphasising the importance of verification and reporting suspicions.

Procurement Policies: Develop clear procurement and payment policies that detail procedures for verifying invoices and supplier information.

Use Secure Payment Methods: Use secure payment methods, such as bank transfers or credit cards, to make payments to suppliers. Avoid using cash or untraceable payment methods, as these are more susceptible to fraud.

Cyber Fraud

Cyber fraud is a common way in which business are vulnerable to criminals. With each year, more sophisticated techniques are used to attack unsuspecting business. In the winter of 2022 – early 2023, it was reported 32% of businesses and 24% of charities recalled any breaches or attacks from the last 12 months. This was much higher for medium businesses (59%), large businesses (69%) and high-income charities with £500,000 or more in annual income (56%).

Cyber fraud encompasses a wide range of tactics and techniques that exploit vulnerabilities in technology and human behaviour. Cyber fraud can take many forms including:

Phishing scams: Phishing is one of the most common types of online fraud in which scammers send fraudulent messages or emails that appear to be from legitimate companies or individuals to trick victims into providing sensitive information such as usernames, passwords, credit card details, or other personal information.

Malware attacks: This is a type of cyber-attack where malicious software, commonly referred to as malware, is used to gain unauthorised access to a computer system or network. The malware can be disguised as legitimate software, such as a software update or a free download, and is typically delivered through email or other messaging platforms, or through malicious websites.

Identity theft: This occurs when someone steals another person's personal information, such as their name, date of birth, national insurance number, bank account or credit card details and uses it for fraudulent purposes.

Statistics show that in 2023, 71% of businesses have a website. The large majority of businesses websites have information about team members with their names, job title, contact information and links to personal social media pages such as LinkedIn. This makes it a lot easier for a scammer to have access to some personal information and images making it easier to impersonate someone.

Online Scams: These include various schemes like lottery and investment scams where victims are promised financial gain or rewards in exchange for upfront payments or personal information.

Business Email Compromise: Hackers impersonate senior executives or employees within an organisation to initiate fraudulent transactions or gain access to sensitive information.
The biggest mistake small businesses make is falling victim to fraudulent emails and human vulnerability. Criminals use simple deception tactics, such as subtly swapping minor details in emails, to deceive employees into sending financial details or making payments. Cyber fraud can lead to financial losses, privacy breaches, reputation damage, and legal repercussions.

Cyber Fraud Prevention

Education and awareness among individuals and organisations are crucial in mitigating the risks associated with cyber fraud. Preventing cyber fraud involves adopting strong cybersecurity practices, such as:

Using Strong Passwords: Use strong, unique passwords for all online accounts and change them regularly. Avoid using the same password for multiple accounts and consider using a password manager to keep track of your passwords securely.

Using the latest software: Keep all software and operating systems up to date with the latest security patches and updates. This can help to prevent cyber criminals from exploiting vulnerabilities in your systems.

Using Anti-Virus Software: Install and regularly update anti-virus software to protect against malware and other types of cyber threats.

Using Two-Factor Authentication: Use two-factor authentication to add an extra layer of security to your online accounts. This can help to prevent cyber criminals from gaining access to your accounts, even if they have your password.

Educating Employees: Educate employees on the risks of cyber fraud and how to recognise and report suspicious activity. Consider using online cyber safe training tools to keep your employees up to date with recent trends.

Backing up your Data: Regularly back up your data to an external hard drive or cloud storage service. This can help to prevent data loss in the event of a cyber-attack or other IT disaster.

Accounting fraud

Accounting fraud, also known as financial statement fraud or corporate fraud, involves deliberate manipulation or misrepresentation of financial information within an organisation's accounting records or financial statements.

The intent behind accounting fraud is often to present a false or misleading picture of the company's financial health and performance. This can mislead stakeholders, such as investors, creditors, regulators, and the public and can have severe legal, financial, and reputational consequences for the organisation and its individuals.

Accounting fraud can take various forms, including:

Revenue Recognition Manipulation: Inflating revenues or recognising revenue prematurely to present a healthier financial picture than reality.

Expense Manipulation: Underreporting expenses or deferring expenses to overstate profits.

Asset Valuation Manipulation: Overvaluing assets, such as inventory, property, or investments, to inflate the company's net worth.

Understating Liabilities: Underreporting liabilities or debt obligations to make the company appear less risky.

Reserves Manipulation: Inappropriately manipulating reserves, allowances, or provisions to artificially enhance profits.

Off-Balance-Sheet Transactions: Hiding liabilities or transactions off the balance sheet to reduce the apparent financial risks.

Improper Disclosure: Withholding or misrepresenting crucial financial information in reports or statements.

Related Party Transactions: Engaging in transactions with related parties at non-market prices to alter financial results.

Fictitious Transactions: Creating fake transactions, customers, or vendors to generate fictitious revenues or expenses.

Inflated Asset Impairment Reversals: Overstating the recovery of previously impaired assets to inflate profits.

Accounting fraud often involves complex schemes and can be perpetrated by employees at various levels within the organisation, including executives, managers, and accountants.

Preventing Accounting Fraud

Preventing accounting fraud requires a combination of internal controls, corporate governance, independent audits, and ethical business practices. Encouraging a culture of transparency, accountability, and reporting of suspicious activities is vital in deterring fraudulent behavior within an organisation.

Conduct Regular Audits: Conduct regular audits of financial statements and operations to identify any signs of fraudulent activity. Consider hiring an external auditor to conduct an independent review of your financial statements and internal controls.

Encourage Whistleblowing: Encourage employees to report any suspicious activity or behaviour to their line manager. Establish a confidential reporting system that allows employees to report concerns without fear of retaliation.

Use Software: Use accounting software that has built-in fraud detection capabilities. This can help detect any irregularities in financial data and prevent fraudulent activity.

Stay up to date with Regulations: Stay up to date with regulations and compliance requirements for financial reporting. This includes accounting standards, tax regulations, and anti-fraud legislation.

Bribery and corruption

Offering or accepting bribes or inducements in exchange for favourable treatment or business opportunities is another form of fraud businesses can be susceptible to. Bribery is a serious crime and have unlimited repercussions on a person or business. It can involve using one's position of power to influence business decisions for personal gain and can take the form of, but is not limited to, cash equivalents, commission, goods, hospitality or training programmes.

Businesses should develop and enforce a code of conduct that outlines ethical practices and behaviour. This should include policies on gifts and hospitality, conflicts of interest, and reporting of any suspected or actual instances of bribery or corruption.

Preventing Bribery and corruption

The Financial Conduct Authority (FCA) has established rules and regulations to combat bribery and corruption in financial services. The FCA's rules on bribery and corruption apply to all financial services firms, including banks, insurers, and investment firms, operating in the UK and requires that firms have robust anti-bribery and corruption policies and procedures in place and implement adequate measures to detect and prevent bribery and corruption within their organisations.

Some of the key requirements set out by the FCA in relation to bribery and corruption include:

Adequate systems and controls: Financial services firms are required to have adequate systems and controls in place to prevent bribery and corruption, including risk assessments, policies, and procedures. These controls should be proportionate to the nature, scale, and complexity of the firm's activities.

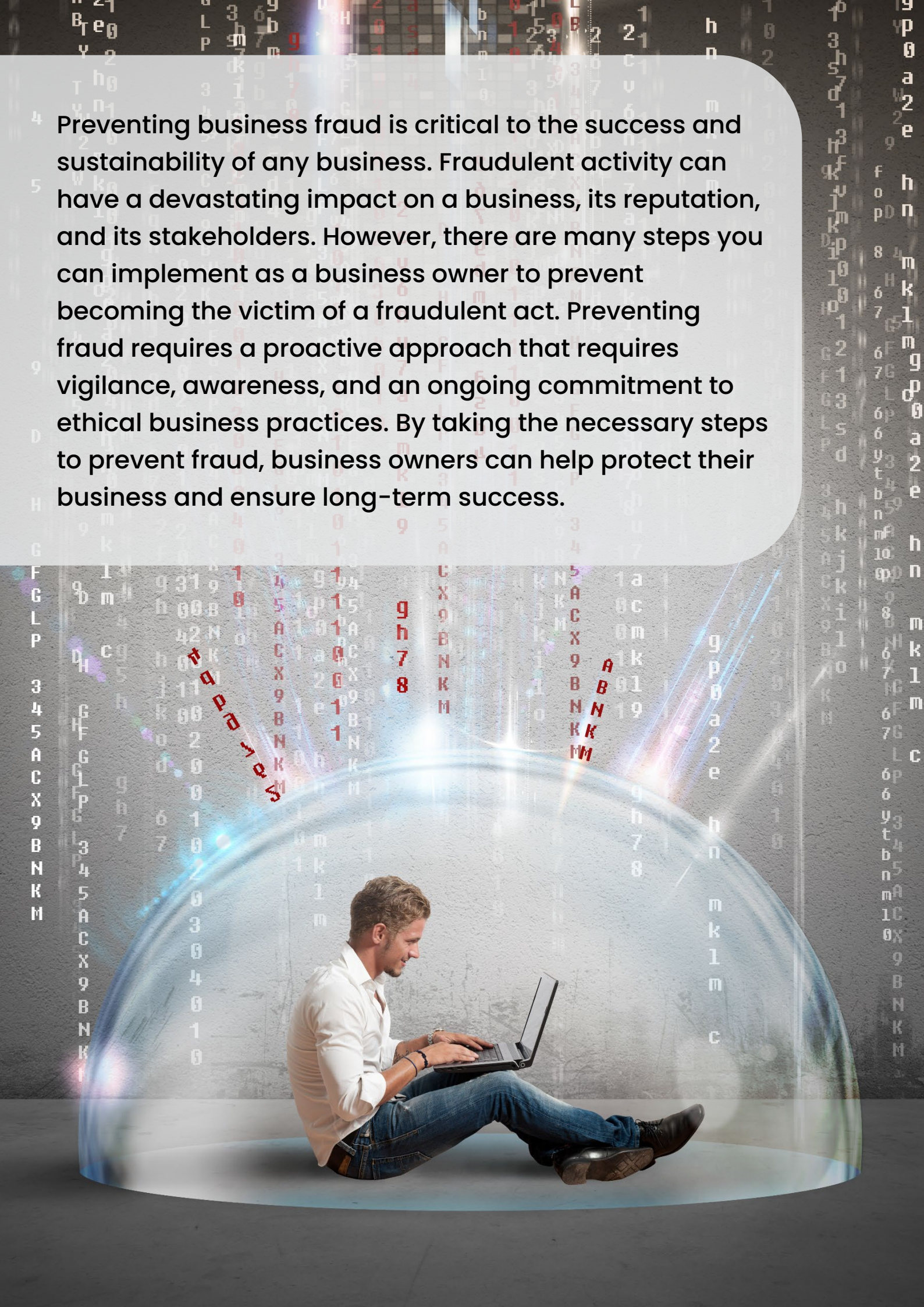
Training and awareness: Firms should ensure that all employees are aware of their obligations under the anti-bribery and corruption policy and receive regular training to ensure they understand their responsibilities.

Due diligence: Firms must conduct appropriate due diligence on their customers, clients, and suppliers to identify and manage the risk of bribery and corruption.

Reporting: Employees should be encouraged to report any suspicions of bribery or corruption, and firms must have procedures in place to handle such reports.

Monitoring and review: Firms are required to regularly monitor and review their anti-bribery and corruption policies and procedures to ensure they remain effective and up to date.

Preventing business fraud is critical to the success and sustainability of any business. Fraudulent activity can have a devastating impact on a business, its reputation, and its stakeholders. However, there are many steps you can implement as a business owner to prevent becoming the victim of a fraudulent act. Preventing fraud requires a proactive approach that requires vigilance, awareness, and an ongoing commitment to ethical business practices. By taking the necessary steps to prevent fraud, business owners can help protect their business and ensure long-term success.



The importance of remaining invested

Tel: 01565 658 840

enquiries@lyncwealth.co.uk

www.lyncwealth.co.uk

Publication date: October 2023