News & Insights

Protecting Your Business From Internal And External Fraud

7 February 2018

Fraud is one of the most common ways for a business to be scammed out of money and no matter the size of your business you can still find yourself a victim of fraud.

Fraud is one of the most common ways for a business to be scammed out of money and no matter the size of your business you can still find yourself a victim of fraud. Not only can fraud have serious financial implications, it can also impact your brand and reputation. In this bulletin, Gallagher explains the types of fraud that can affect your business, how to report instances of fraud and the kinds of insurance that can help your business recover should an incident occur.

Just how big a problem is fraud for businesses?

Fraud can be a massive problem for businesses and as they become increasingly digitalised, the problem is only likely to get worse. The Annual Fraud Indicator 2017 stated that annual UK losses to fraud are estimated at £190 billion with £140 billion of that coming from the private sector. For the private sector, one of the most common of these are procurement and payroll fraud, as these can be easy to manipulate by insiders. This is followed by financial sales fraud such as online and telephone banking scams. Another area to consider is cyber-crime, of which there were 3.6 million reported cases of last year.

What types of fraud are there?

As described earlier, claims usually involve someone within or outside the organisation and below are some examples of each – as you can see some could emanate from either.

Internal Fraud Examples

- Fraudulent cheques
- Misuse of credit cards by staff
- Staff claiming false or inappropriate expenses and being reimbursed by the business

- Director, Finance Director, Head of Counter-Fraud and similar high ranking officials stealing monies raised and released through payments made to fictitious organisations
- Sale of land or property by an employee who then fails to pass on all of the sale money
- Temporary staff in finance or other departments allowing organised crime access to financial data
- Inadvertent human error through email, file sharing or USB sticks being lost

External Fraud Examples

- Fraudulent cheques and false invoices
- Identity fraud by hijacking bank accounts or phishing emails
- Card-washing schemes – using online payment systems to test a stolen credit card
- Hacking and theft of databases that can be sold on to third parties to mine
- Email purporting to be from Chief Executive requesting sensitive information or transfers of funds. Usually achieved by cloning email addresses so they appear genuine unless carefully scrutinised
- Temporary staff in finance or other departments allowing organised crime access to financial data

What are the warning signs?

- Most fraud can be caught by internal controls or audit processes so make regular checks on accounts and records and look for warning signs
- People commit fraud for a range of reasons – debt or greed, boredom, as a search for status or simply just through opportunism. Be alert to changes in behaviour.

Preventing fraud

With recent Government statistics revealing that fraud affects 1 in 4 small businesses every year , it's no wonder that many organisations are looking at strategies to combat this growing problem. It isn't just cyber crime either, with the losses from payroll fraud estimated at £12.7 billion for private firms.

The Government's advice on fraud and crime states that while all businesses are vulnerable to fraud and financial crime in some way, those who do not have the correct financial controls in place are putting themselves at needless additional risk. Your organisation needs to have an appropriate set of financial controls in place, which should be tailored to the size of your organisation. Naturally the larger your organisation, the more important it is for your business to implement a broad set of anti-fraud measures.

Action Fraud suggests the following steps to help prevent fraud:

1. Know your employees – internal threats can come in many forms so it's important that you can trust your staff. Always ask for at least two references when taking on new staff and verify their personal information wherever possible.
2. Know your customers – assess each customer's profile and the transaction they are requesting. If a transaction seems suspicious then trust your instinct and don't be afraid to request further information or proof of address.
3. Know your suppliers – make sure you take the time to verify that they are who they say they are, and to research their reviews online. Double-check your invoices so that you know you are getting the goods and services you are paying for and always keep an eye on their financial health.
4. Know your assets – identify and monitor your assets, only giving access to the necessary employees. This applies not just to tangible assets but also data and intellectual property.

This positive pre-loss approach clearly could save businesses thousands of pounds and it has to be said a lot of this advice is out there and is fairly simple to implement.

Reporting fraud

If you suspect that fraud has been committed against your business, your first step is to report it to Action Fraud – not only do they offer 24/7 crime reporting for businesses, but their business reporting tool speeds up the process by helping you to provide the correct information for single and multiple cases of fraud and cyber crime. You can contact Action Fraud using their online form **https://www.actionfraud.police.uk/report_fraud (www.actionfraud.police.uk/report_fraud)** or by calling **0300 123 2040.**

Of course, if the fraud relates to online banking, cheques or debit cards or you suspect fraudulent activity on your account, contact your bank or Credit Card Company.

The Fraud Advisory Panel suggests common options for recovering fraud include:

- Criminal and civil proceedings
- Insurance claims
- Action taken by regulatory or professional bodies
- Action taken by your bank

Conviction statistics for fraud are generally high with 94% of perpetrators convicted through the City of London's Dedicated Card and Payment Crime Unit. You can opt to sue the fraudster through the civil courts where there is a lower standard of proof and these courts can offer speed, control and flexibility. But it can cost quite a bit of money to go down this route so think carefully.

Insuring your business against fraud

Recent statistics from Action Fraud state that fraud affects 1 in 4 small businesses every year and that last year fraud losses to SMEs were estimated at £18.9 billion. Fraud can affect any business no matter what size and with so many types of fraud potentially emanating from inside and outside the business, it can be hard to predict and prevent. That's why you need a robust insurance policy, so that if the worst does happen your business can get back on its feet with minimal damage to your revenue, reputation and long-term financial health.

There are two types of insurance available:

- For internal fraud - Fidelity Guarantee or Employee Crime only
- For internal and external fraud – Crime Insurance

The former was the first type of cover available and has been around for over 40 years. It offers protection and compensation should a business be defrauded by its finance director, employee, or temporary worker, amongst others. There are usually standardised limits available, some from as low as £25,000 for small businesses with minimal/petty cash style exposures, through to £5m and £10m limits for larger businesses that have numerous financial transactions going through on a daily basis.

Fidelity Guarantee insurance usually has excesses that relate back to the limit so whereas a petty cash style cover with a £25,000 limit might only have a £500 excess, a full-scale £1m limit employee crime policy is likely to have an excess of £5,000 or £10,000.

The wider Crime cover extends to cover fraud involving the public, organised crime, temporary workers and anyone else that is not part of the business. Such cover may also include computer based theft such as third party computer fraud and electronic funds transfer fraud.

Once again cover is usually available at standardised limits and with proportionate excesses to avoid small claims being processed as this is not what the insurance policy was developed to cover.

Technology based fraud can also be covered by a Cyber Policy so it is important to make sure you don't end up with dual insurance – but bear in mind the fraud MUST involve a cyber/non-manual risk to trigger.

The insurance market sees hundreds of claims each year, some internally driven and some externally, including those involving organised criminals looking for an easy target.

Many insurers can offer support in terms of free advice on improving fraud risks and minimising impact once an incident is notified. This sometimes occurs at proposal stage when an underwriter may want to encourage a business to change a procedure that it believes leaves them open to fraud.

Case Studies

The following examples show how easily fraud can cause problems for your business – and what the consequences could be.

Mandate Fraud

An employee receives a phone call from an individual who they believe to be a genuine supplier saying that their bank account has changed and payment is to be made to a new account.

Going through procedure, they advise the request must come in writing via email or on company letterhead. The employee later receives an email from what appears to be the supplier complete with the supplier's signature at the foot of the email. The employee proceeds to change the bank details and payment is issued. Sometime later, the genuine supplier requests payment, indicating that the original payment was never received. Further investigation will identify that the requests were fraudulent.

Fake President Fraud

A mid-level finance employee is the only one left in the office on a Friday evening and receives a phone call from an individual who identifies himself as the CEO of the company. He explains that there is a major acquisition about to take place, it must close tonight and he can't get hold of anyone else in the finance team to process the payments.

The employee explains that she only has limit to transfer funds up to £50,000 and no one else is still in the office to countersign the transfer. The CEO grows more irate with the employee who is refusing to transfer the funds because she does not have the authority, repeatedly telling her he's granting the authority. Eventually the CEO persuades her to circumvent the established procedure by issuing multiple £50,000 transfers, totalling £500,000. It later transpires that the call was fraudulent.

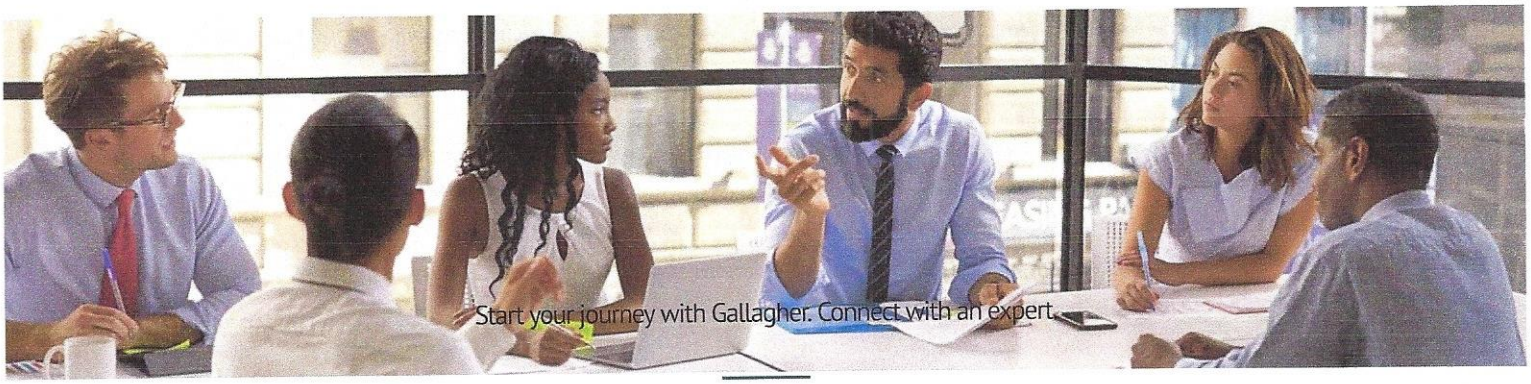
Employee information compromised

The insured became aware that a number of its employees were being subject to tax fraud – tax refunds had already been secured in their names. Supported by our breach response team and external forensic teams, the insured confirmed their systems were secure and the cause was likely an external provider.

Ransomware

An insured's employee clicked on a malicious link which resulted in the download of a CryptoLocker ransomware - malware that encrypts the system it attacks and demands payment to release.

Assisted by our breach response team and external forensic teams, the insured's internal team was able to restore elements of the compromised data, but the issue resulted in paying over £5,000 in extortion payments using a cryptocurrency – which insurers have covered.



Communication Consulting (https://www.ajg.com/uk/communication-consulting/)
Employee Benefits (https://www.ajg.com/uk/employee-benefits-consulting-overview/)
Rewards Consulting (https://www.ajg.com/uk/reward-consulting/)
Financial Planning (https://www.ajg.com/uk/financial-planning/)

Claims (https://www.ajg.com/uk/personal-insurance/home/)

Claims Management (https://www.ajg.com/uk/corporate-insurance/business-assist-claims-management/)

About Gallagher (https://www.ajg.com/uk/about-us/)

The Gallagher Way (https://www.ajg.com/uk/about-us/the-gallagher-way/)
Gender Pay Gap Reports (https://www.ajg.com/uk/about-us/gender-pay-gap-reports/)
Investor Relations
Locations (https://www.ajg.com/uk/office-location/)
Premiership Rugby Partnership (https://www.ajg.com/uk/rugby/gallagher-premiership-rugby/)

TOP

Contact Us (https://www.ajg.com/uk/contact-us/)
Privacy Notice (https://www.ajg.com/uk/privacy-policy/)
Cookie Policy
Legal & Regulatory Information (https://www.ajg.com/uk/legal-and-regulatory-information/)
Modern Slavery (https://www.ajg.com/uk/about-us/modern-slavery/)