Graydon Report

External Business Fraud in the UK

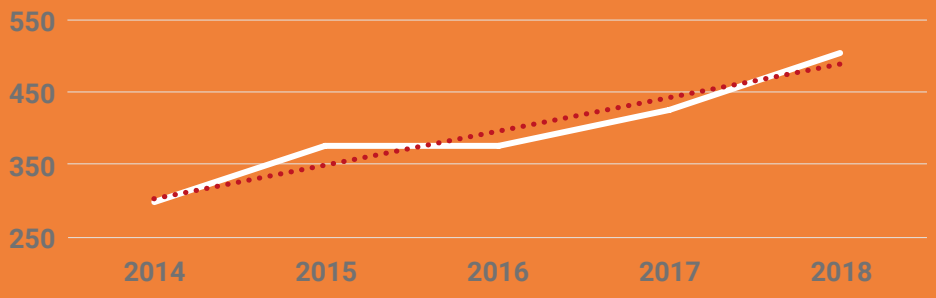
GRAYDON
open in business

Graydon's Fraud Investigations

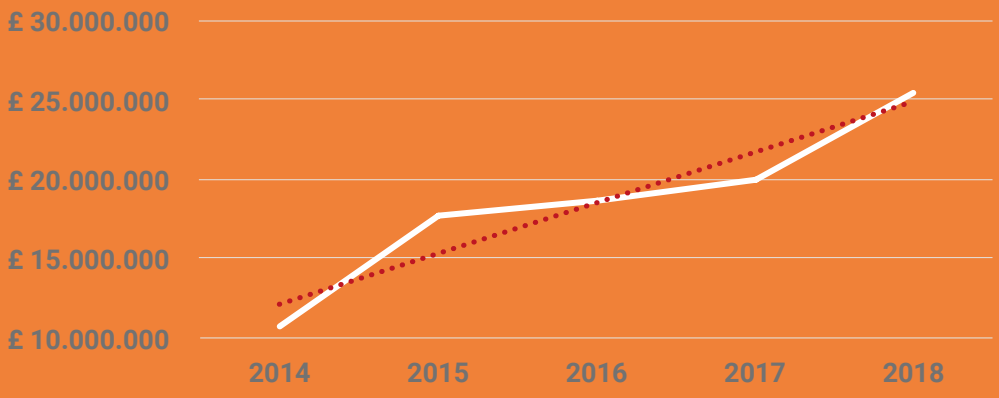
- £ 0.5 million of suspected frauds identified every week
- £ 250 million identified over last 15 years
- 28% increase in volumes from 2017 to 2018
- £29 million recognised losses (CCJs)
- Average loss (CCJs) - £7000

Volume cases at highest level since the Financial crisis

Volume of Suspected Fraud Cases indentified by Graydon



Value of Suspected Fraud Cases indentified by Graydon



External Business Fraud in the UK: An Overview

1. Introduction

Fraud is a constant in commercial life. In the UK, we've had laws to protect us since 1275. The only difference these days is that technology has expanded both the fraudster's repertoire and the preventative measures you can take.

You can find many definitions of fraud, especially in the legal literature, but some are more simple than others. Action Fraud simply declare: "Fraud is when trickery is used to gain a dishonest advantage, which is often financial, over another person." The Chartered Institute of Management Accountants offers a similar definition: "Using deception to make a personal gain for oneself dishonestly and/or create a loss for another."

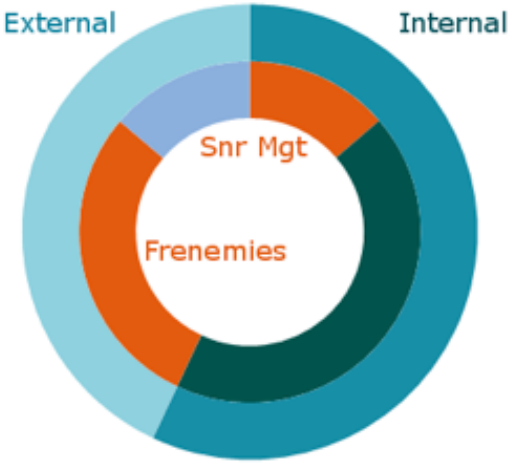
The best two current estimates place the annual cost of fraud to UK businesses at between £106bn and £140bn per annum. This is a largely unnecessary cost because companies can prevent much of it. Indeed, it should form part of the firm's overall risk strategy that should, in turn be a board level responsibility. After all, the board is accountable for the company finances and its conformity with laws and regulations.

From a company perspective, fraud instances can be either internal or external. If you have business partners or customers connected to your system then, from a fraud management perspective, they ought to be treated as 'insiders'. However, a high percentage of reported frauds are by these 'frenemies'. The following illustration is based on PWC's Global Economic Crime And Fraud Survey 2018 report.

Most internal fraud is prevented or detected by internal controls or audits and alerts from customers, staff and whistleblowers. External fraud requires a different approach: one based heavily on prevention.

Law enforcement is responsible for discovering a tiny minority of frauds of all kinds. The authorities do not have the interest or the capacity to address the vast majority of fraud activities (around 90 percent at the last count. Source: Graydon). You have to deal with fraud yourself.

This report focuses on external fraud – attacks from individuals and organisations that are beyond the perimeter of your business. It introduces you to the types of external business fraud and the consequences for your business. It then looks at a set of very practical preventative measures that will vastly reduce your exposure, including links to helpful resources. Finally, it looks at what to do if you detect a fraud and the laws that exist, should you decide to track down and prosecute the perpetrator.



Internal vs. External Fraud showing some significant perpetrators (the unlabelled bars are 'others')

2. Executive summary

The costs of fraud are not just the immediate economic and reputational impact. They also include fines from regulators and the costs associated with investigations and, maybe, prosecutions through criminal and civil legal processes. Prevention, in the case of fraud, is better than an expensive cure.

Thanks to GDPR and other upcoming legislation, the business and legal climate is increasingly moving towards 'transparency' in which organisations are encouraged to share and publicise successful frauds. While this may be helpful in a collective intelligence sense, it has to be managed carefully to avoid serious reputational harm both internally and in the outside world.

Fraudsters will always exploit new weaknesses and invent new scams to breach your defences. Attacks boil down to: abuse of trust, confidence tricks, forgery and theft. Prevention is largely in your hands. Or, to be more accurate, in the hands of your staff. They are the guardians of the company perimeter.

Make sure that someone is responsible for checking that your own website has not been tampered with. It's not unknown for a successful fraudster to redirect website links to similar-looking but entirely fraudulent destinations.

Education and training are the starting point. Awareness for everyone and training in security measures for those responsible for vetting credit applications, tenders, contracts, purchase orders, invoices, and so on. This extends to third parties if they are within your security boundary. The whole initiative needs to be visibly and actively supported by the board and to harmonise with any existing security initiatives.

Fortunately, connection to the internet means that many online resources are available to your staff for checking individual and company credentials. They could even use Google Street View to take a virtual trip to check out a supplier's premises.

Just as you have a formal credit policy, make sure you have documented a fraud prevention policy. And keep it up-to-date. The two should be complementary.

In the event that fraud is detected, three actions are important:

- **stop the activity immediately**
- **collect and store evidence safely**
- **contact the nominated security specialist**

At this stage, it is best to say nothing to anyone else for fear of alerting the fraudster or a collaborator. The specialist will then take control of remaining actions and notifications.

If you are considering civil or criminal legal action, take legal advice and weigh the costs of action versus inaction very carefully. If the fraud has resulted in the theft of personal information then it's unfortunate but, under the terms of the General Data Protection Regulation, you are obligated to report it. Heavy fines can be levied on companies in breach of this law.

The remainder of this report will take you into more detail of the possible external frauds and the preventative and remedial measures you can take.

3. Consequences of external frauds

Successful fraud will always leave your company out of pocket. It could be, for example, a fraudulent transaction, a deliberately unpaid bill or confidential information shared with a competitor. Apart from a direct financial impact, if your firm is found responsible for allowing the fraud to happen, it could face fines or legal action. The distraction of an investigation and preparing your defence can add significantly to the cost of the original breach.

The overall impact of a successful fraud will depend on its size and the degree to which it becomes publicly known. Many companies are notoriously reticent when it comes to sharing information about breaches of their fraud and other security defences. This is becoming more difficult as the business climate changes towards greater transparency and mandatory notification regulations are being introduced.

External fraud affects different communities in different ways. Here, we examine the impact of a fraud on your company on insiders, investors, authorities and the general public.

Insiders

The number one consequence of all frauds is financial loss. Its effect could be felt through lower investment, lower growth, lower salaries and fewer perks.

Internal morale can be affected, resulting in a general atmosphere of embarrassment and annoyance, especially if salaries are affected. (This report doesn't cover deliberate fraud by insiders but, were it the case, you could add 'a general atmosphere of suspicion' to the list.)

A badly-hit company could declare itself insolvent and create the potential of a return to profitability.

In extreme cases, a fraud could even cause a business to collapse.

Investors

One of the reasons companies try to keep a lid on fraud is in order to maintain investor confidence and avoid embarrassment. This is actually a fraud against the investor.

Authorities

If a fraud caused your company to be subject to a legal or regulatory investigation, your day-to-day operations could be severely disrupted. A resulting legal battle could become an expensive further distraction.

General public

Once word gets out about you becoming a fraud victim, especially if it results in harm to your customers, suppliers or other business partners, this magnifies the impact on your credibility.

Adverse publicity is probably top of the list. You are marginally better off if you are the source of the story. A leak is more damaging than a confession, but both can be harmful to the reputation of your company name or your brand. Well-known brands have recently experienced it.

If customer confidence is weakened, then sales could be impacted, leading to some of the financial problems mentioned earlier.

Plus, other fraudsters might consider you a likely target, knowing that you've already fallen victim at least once.

4. Types of external fraud

Corporate fraudsters are well practised in the arts of deception and they're always looking for new ways to extract money from the unwary. Whether old or new, the frauds can be considered under four main headings: Abuse of trust; Confidence trick; Forgery; and Theft. As frauds and fraudsters themselves are always evolving, these are only a sample of current types of fraud.

Abuse of trust

Having established trust with your company, an outsider then exploits it to steal money or other assets from you.

Short firm fraud: A business places several small orders with you and pays promptly for each one. This clean, albeit short, track record leads you to accept a large order. It would be in easily-traded and hard-to-trace goods. You deliver and that's the last you hear from them. It could well be that they also secure up-front payments from their would-be customers, thus defrauding them as well.

Insolvency-related: Companies trading immediately before they know they're about to be declared insolvent.

Illegal trading: Directors who continue trading while suspended or disqualified.

Confidence trick

Procurement fraud: Fraudsters issue false invoices (en masse) to extract payment for goods or services that either do not exist or turn out to be of inferior quality.

CEO fraud: Someone in the purchase ledger department gets an email, apparently from the CEO or managing director, authorising an urgent money transfer.

Forgery

Company hijack: A fraudster files fresh address and director details for an existing company at Companies House, thus inheriting that company's credit-worthiness.

False filing: Before applying for credit, a fraudster files false accounts and other documents at Companies House.

False accounting: A company's financial position is misrepresented to make it look more attractive to would-be financiers, investors, suppliers or customers.

Phoenix company: A director puts a company into liquidation to avoid paying its creditors. The director then starts a similar new business, buying the assets of the original company for less than their actual value.

Carousel fraud: The fraudster acquires a VAT number in order to buy VAT-free from other EU member states then sell at VAT inclusive prices, finally disappearing without paying the VAT owed. They often don't deliver the goods either.

Theft

Copy/Steal: Digital information can be copied with little evidence of your loss. Both digital and physical assets can be stolen.

Fake identity: A fraudster uses another person's identity (real or imaginary) to obtain goods or services.

Stolen ID: Steal security information in order to masquerade as someone else. Details are usually obtained through an authentic-looking email that appears to be from an organisation you trust.

Using the assets or information of an organisation for unofficial purposes. This is especially true if your company shares confidential information outside (business partners, service providers ...) because, without strong internal controls, the fraud is invisible.

5. External fraud prevention

The good thing about preventing external fraud is that a company can take many of the steps easily using manual procedures. It's about discipline and developing a sense among all the staff that they are responsible for keeping their guard up, even as the uptake of automated support tools increases (see chapter 8). The driving force should be someone at board level, even if they devolve implementation to other authorised and credible members of the executive team.

Don't expect much help from the authorities beyond advice. Unless a fraud is extreme, they're unlikely to be interested.
At heart, your prevention measures boil down to effective education, training, augmenting manual processes as appropriate, and access to sources of help, many of them online. You need a fraud incident plan that identifies the steps to take in the event of a fraud attempt or, indeed, a successful fraud. It identifies the roles needed to swiftly take action and nominates and trains those responsible. This will form part of your wider fraud management framework, which will include awareness, education and training targeted according to the employees' (and business partners') roles in protecting your company from fraud.

These efforts should be closely aligned to the work of your other security teams (information and, increasingly, cyber). If these do not exist, then you are laying yourself wide open to other kinds of internal and external attack.

Everyone who has access to your confidential information needs to be aware of the possibility of fraud and their role in preventing it. They could be inside your company or among your business partners, suppliers or customers.

Preventative actions

Whenever you get a new client, a credit application or an unusually large order, make sure you check every detail. Never accept the information they give you at face value. Here are some of the main elements that you need to check and monitor in order to minimise your exposure to fraud:
Check credit applications

Double check every detail of the credit application form. Look for omissions and lies. Check that the delivery address actually belongs to the company and be deeply suspicious of PO Box addresses. You may be able to check the authenticity of the email addresses – an email server that accepts a wildcard match for the text that precedes the @ will show as 'unverifiable'.

Check premises

Meeting the client face-to-face on their own premises is hugely reassuring but not always practical. Google Street View can be a great help if you can't visit. You need to supplement this with other checks that can be done by telephone or online. Ask neighbours about them or, if their premises are leased, their landlords. Your aim should be to seek evidence of long-term occupation and their general credibility. Some companies take a short-term lease in order to defraud as many businesses as possible before moving on.

Even from Google Street View, you can generally tell whether their premises match their type of business.

Check identity

A visit to the Companies House search facility gives you access to a wealth of useful information on limited companies including registration documents, financial health, trading history, company directors, addresses and auditor information. The registration number is the one company data item in the UK that can never change. However, bear in mind that Companies House simply files the documents supplied. It is your responsibility to decide if the information is genuine.

A good first check would be to see if their auditor is registered with a recognised professional audit body. You may be able to spot filing anomalies such as the same signatures appearing under different names in successive annual returns. Look at the filing frequency: is there an established pattern or are there fluctuations in timing or financial figures? Suspicion is your only safe attitude while doing this work.

It's easy to check whether their VAT number is genuine by going to the VIES VAT number validator.

Check out their auditor

Check how many companies they audit and, if the list is short or the clients mean nothing to you, see whether connections exist between them. Maybe their clients share the same directors, for example. Apart from the auditors' own lists, Adviser Rankings Limited provides lists of quoted clients for many auditors.

Monitor behaviour

When a company starts behaving differently, it may be a sign that they are no longer who they claim to be. Perhaps their order patterns are different or they've changed when and how they contact you. Any variation from what you consider normal should be a signal to investigate. Consider joining or attending intelligence networks for your industry where you can exchange useful information on clients and prospects, long before it becomes public knowledge.

Check individuals
Check out the directors. Companies House records show their other directorships and sometimes give enough personal information that you can look for them on LinkedIn or using a general web search.

Check web presence
Apart from the obvious step of visiting their website, check the ownership of the domain name. This is easily done starting with the whois.net or similar service. This reveals historical information as well as where you can find deeper information, such as names and addresses of the people involved - follow the link next to the 'Registrar WHOIS Server' entry. With the massive increase in 'top level domains', it's easy for a fraudster to buy a convincing sounding domain name e.g. sainsburys.biz

Handling transactions
First of all, limit the responsibility of paying bills to one or two staff members, this gives you control and narrows your exposure. In any event, they should never feel pressured to pay an invoice, no matter who's pushing. They need to check every detail of the supporting documentation, including the small print, which may be on the client's website with a link in the invoice. (They need to check that the link isn't taking them somewhere it shouldn't before clicking on it.) They need to check that the order and invoice details match and that the delivery address matches the one on file.

Follow your tender process
Bid rigging and payments are the primary opportunities for external fraud in the tendering process.

The Government's www.gov.uk/cma site gives lots of relevant advice on bid rigging. Use the search box and don't be put off by the public sector focus.

At the time of payment, check all the documentation. Vague invoice descriptions, round amounts and price changes are all clues to potential fraud. Make sure you know the delivered goods are of the promised quality before releasing funds.

Monitor clients and prospects
Someone has to monitor all your clients' filings and public statements. If you have the resources to do this, fine. If not, it's worth paying someone else to do it. A recent change in a public filing could be the clue that someone's about to commit a fraud. In any event, you'll need the new details.

An unusual number of documented changes in a short timeframe should be considered warning signs. These changes could include new director appointments, delivery address changes, an unusual improvement in company performance, many credit checks in quick succession or filing new accounts quickly after the year-end (most companies don't).

Know everyone
It's vital that you know your customers, suppliers and the other third parties you transact with. And bear in mind that their circumstances may change. Keep an eye on the wider market picture because businesses that have thrived in the past may not be doing so well today – you can just look to the turmoil in restaurant and retail chains for everyday examples.

Third parties can help you
Credit reference agencies can help in a number of ways. They can spot Companies House filing anomalies. They can provide company snapshots and they can continuously monitor companies for changes in status, credit ratings, contact details, directors, registered addresses, and so on.

Education and Training
An education programme raises awareness among all staff and business partners of the risks of fraud and the likely opening gambits of the fraudsters. It encourages vigilance. Training goes deeper for those who need it; it goes into the details of precautionary actions and gives staff practice at taking preventative measures. Your programmes will be underpinned by two policies – one on credit and the other on fraud. It needs to fit in with your wider information security programme that may, in turn, be part of an even wider cyber security programme.

Fraud Policy
Your fraud policy will cover internal and external fraud. Plenty of sample policies exist if you don't have one. As far as external fraud is concerned, the policy needs to make clear who is responsible for managing fraud, the procedures employees should follow in the event of suspected fraud and who is responsible for preserving evidence, notifying the authorities, regulators, affected stakeholders and, possibly, the media.

Credit policy
Your credit policy will work hand-in-glove with your fraud policy and will include guidelines on how to decide which companies will be given a credit line, their credit limits, their payment terms and how to deal with defaulters. Its aim is to encourage new business through decent credit terms while, at the same time, protecting the company's commercial interests.

Finally
Check that your own business filings and websites have not been tampered with to create an advantage for a fraudster.

6. Detection and action

Your strong prevention measures should limit your exposure to fraud. However, no system can protect you against all frauds all of the time. If an employee suspects that a fraud is in progress, their first duty is to stop the activity or transaction they're engaged in and, if they can, prevent further incidents.

Their second task is to notify the assigned fraud contact in your organisation. They will know who this is from their fraud awareness training. They might be tempted to report it to their boss and let them take matters further. This is okay as long as they are absolutely certain that their boss has no involvement in the fraud.

At this early stage, it is very important that as few people as possible know what's happening. Once word gets out that a fraud has been unearthed, the perpetrators will try to cover their tracks. We include this under External Fraud because it sometimes requires collusion from an employee.

Evidence

The company will need evidence of the fraud and, guided by a member of the security team, your employee needs to gather it without alerting the fraudster of their discovery. Whatever they gather – fake invoices, payment transfer requests, and so on – must be stored somewhere the fraudster can't get at it.

If the fraud is part of a major crime – money-laundering for example – the authorities could well investigate your company's involvement, even if you are innocent of wrong-doing. Two things will make life easier for you: the fact you have followed a fraud incident procedure, and the fact you have captured incriminating evidence.

Share

The reasons for non-disclosure are many but the main ones are reputational harm, creating a magnet for further fraud, the distraction of an enquiry, and the feebleness of the subsequent punishment. Most companies would prefer to swallow the loss and tighten their fraud control procedures. However, keeping quiet about fraud is generally not a good idea. Better to manage it and plan how to communicate the story both internally and externally. Internally may be in the form of an update to your fraud awareness, education and training programmes, to reduce the chances of a similar fraud being successful. This would also include praise for the person who spotted the fraud and reassurance that the company is okay and their livelihoods aren't threatened.

Report to Action Fraud, the UK's national fraud and cyber crime reporting centre and consider sharing the news in your industry groups, to encourage others to be on the lookout for similar activity. Bear in mind that, another time, a report from an industry peer could help you too.

7. How automation helps

Successful fraudsters are continually evolving and advancing their attack techniques. They have to, because their target organisations keep improving their own anti-fraud measures. Increasingly, each side is using automation as a way of leapfrogging the other.

The third-party route

The best way to introduce meaningful automation into an organisation is to integrate third-party fraud-spotting systems into their business processes. The good suppliers are able to share their algorithm development costs among many customers. They are also able to sign up for many sources of data and insights – the fuel that drives their detection systems. The best ones will incorporate fraud information gathered in real time from their customer communities. Some will go a step further and create a community of business intelligence suppliers with common but complementary interests, all making their specialist data and services available through a single platform.

The IT department of any company, no matter how big, would find assembling and maintaining such an infrastructure a quite impossible task. This feat is far more achievable and more efficient were it to purchase such a solution 'off-the-shelf' whenever possible.

Humans and automation

Ideally, for the customer and the service provider, the customer needs to be in control. They need to define their needs, choose from the data and services available and create or adapt the fraud-checking 'journeys'. The user interface needs to be simple – drag and drop ideally – so they can easily map journeys and act on the decisions that emerge, either by triggering another journey (accept/reject in the case of a credit application) or by referring to a human or a team.

Assuming the service is cloud-based, decisions and actions can be made in near, if not real time.' Human involvement should be minimised, being called in only when an exception condition is referred. It is important that this referral is completely transparent and understandable to the human, rather than a black box "because the computer says so" referral.

The service provider's decision-making steps will all be transparent in the first instance so the client can check the audit trail and provide vital feedback to the developers. For some activities, if the decisions offered are consistently reliable then they might be automated end-to-end. E.g. In the case of the credit application the accept/reject notification could be sent and only referrals would make it through to a human for validation.

Machine learning

Service providers will use machine learning or, possibly, its more clever offspring, deep learning, according to what data 'fuel' is being used. Machine learning parses and learns from data sets and makes decisions accordingly. If flaws are found in the decisions, human intervention is needed to refine the process.

Deep learning goes a step further, using a diet of 'big data' which it absorbs to build continually-learning neural networks. It can present conclusions and refine its logic in the light of fresh evidence from the field. In other words, it thinks for itself. The sheer volume of data is beyond a human's ability to process.

This is the kind of learning that Google's DeepMind AlphaGo used to beat the world's number one 'Go' player. This version was, in turn, beaten by a newer version that learnt Go by playing against itself. However, this kind of system does carry the aforementioned risk of the "computer knows best" and should not be embarked upon lightly.

The benefits of automation

The main benefit, when it comes to fraud, is that companies are able to maximise their protection through automation. Decision-making will be more complete and, often, executed in seconds.

Automation brings many benefits to the business as a whole, fundamentally delivering a better service to its customers while complying with legal and regulatory obligations.

Its business efficiency and productivity benefits include:

- Less human error/improved accuracy
- Faster delivery of results through automation and simultaneous processing
- Refers only exceptions to skilled humans for 'offline' processing

The business outcomes it delivers:

- More informed decisions through automated business intelligence
- Better customer service through improved quality, accuracy, relevance and speed
- More competitive, especially for 'first movers'

Conclusion

UK businesses are under a continuous and growing threat of sophisticated fraud attacks. A blend of automation and human talent provides the best opportunity to fight back. A federated approach where companies combine their knowledge and information sources, makes life even more difficult for the fraudsters.

According to Financial Fraud Action UK, "As a result of investing in advanced detection systems, organisations can prevent £6.40 in every £10 of attempted fraud." Some automation companies believe this figure is unnecessarily modest, suggesting that up to 80 percent of fraud can be detected. When you consider the size of the fraud problem, this would represent a significant boost to the financial health of any company that embraces automation.

8. Sources of help

Help comes in many forms. Some is written for your benefit, some is neutral and much is intended to benefit the organisation writing it. That doesn't make it less useful, it might be worth checking multiple sources. In this case, we're talking about fraud consultants, insurance companies, law firms, and so on.

The online resources mentioned earlier are:

- Action Fraud www.actionfraud.police.uk is the UK's national reporting centre for fraud and cyber crime. It is also a source of news and advice.
- Adviser Rankings adviser-rankings.com provides comprehensive information on corporate advisers (including auditors) and their UK-quoted clients.
- Chartered Institute of Management Accountants (CIMA) www.cimaglobal.com contains fraud-related articles and advice.
- Companies House www.gov.uk/get-information-about-a-company provides detailed information on companies registered in the UK.
- Competition and Markets Agency http://www.gov.uk/cma/ provides information about, among many other things, bid-rigging fraud.
- Credit Reference Agencies e.g. www.graydon.co.uk provide detailed and actionable intelligence about the businesses you deal with.
- Expand short URL www.checkshorturl.com is an example of the many services that expand a cryptic web address to the full version.
- Financial Fraud Action UK www.financialfraudactionuk.org.uk provides a forum for members to work together on non-competitive issues relating to financial fraud.
- Google www.google.co.uk/maps/ lets you 'visit' addresses using the Street View option.
- LinkedIn gb.linkedin.com provides self-authored details of individuals, mainly business people
- VAT number validator ec.europa.eu/taxation_customs/vies/ allows you to check whether any EU VAT number is genuine.
- Who Is who.is reveals details of who a website belongs to. Sometimes people elect to hide their details, but it's worth a try.

Other sources of help:

- Archive of all UK laws www.legislation.gov.uk
- Fraud Advisory Panel www.fraudadvisorypanel.org provides information, education, training and research into fraud.
- National Cyber Security Centre (NCSC) www.ncsc.gov.uk is a central resource for most information on cyber security and related issues.
- A unified fraud detection, identity and compliance platform is offered by Graydon technology partner TruNarrative trunarrative.com

9. Criminal and Civil Law

Like the bolted horse when the stable door is left open, by the time many frauds are detected, the perpetrator is long-gone with their ill-gotten gains. The chance of conviction and reparation has to be considered at board level together with the potential cost, disruption and publicity of civil or criminal action. Seek and listen to legal advice before embarking on any action.

"The legal sector's challenge is to keep pace with the rapidly changing methods by which the ever more sophisticated fraudsters trick their way into obtaining payments through online scams and false accounting."

Ward Hadaway
one of the UK's Top 100 law firms

Prevention, in the case of fraud, is unquestionably better than cure.

The primary relevant laws are the Fraud Act (2006), the Theft Act (1968) and the Computer Misuse Act (1990).

Fraud Act

When it comes to external fraud, the offences under the Fraud Act centre around the perpetrator's intent to make a gain for himself or another, or to cause loss to another, or to expose another to a risk of loss. One way is to make an untrue or misleading representation, knowing it to be false. The other is to dishonestly fail to disclose information that they have a legal duty to disclose.

Another offence is fraud by abuse of position. In the case of external fraud, this is less likely than a fraudster claiming to be someone they aren't.

Theft Act

Under the Theft Act, a person is guilty if they dishonestly appropriate property belonging to another with the intention of permanently depriving the other of it. Motivation is irrelevant. Some clauses in the Act were superseded by the Fraud Act. False Accounting remains, however. This is where a person dishonestly "destroys, defaces, conceals or falsifies any account or any record or document made or required for any accounting purpose; or in furnishing information for any purpose produces or makes use of any account, or any such record or document as aforesaid, which to his knowledge is or may be misleading, false or deceptive in a material particular". This could be the case when an employee colludes with an external party.

Computer Misuse Act

This Act refers to unauthorised access to computer material. Whether successful or not, this is an offence. In the case of external fraud, it relates to the means by which the fraud is executed. The fraud itself would be prosecutable under the Fraud Act. Some parts of the Fraud Act not mentioned earlier, relate to making, supplying or possession of 'articles' for use in fraud. To untangle the best course of action it is important to take legal advice.

Civil Remedies

A civil action is faster, requires a lower standard of proof than a legal action, you have more control over the process and it focuses on recompense. The law enforcement agencies focus more on securing a criminal conviction and they may need several reports of a particular type of fraud before they take action. You could, in theory, pursue both routes in parallel, or pursue the civil route if the legal one fails. This could end up an expensive, time consuming and distracting process, so you'd have to be fairly sure that you'd win your case(s). Once again, legal advice is vital.

Civil law provides for many actions against multiple personae, for example: the perpetrator, whoever now has the stolen assets or a professional advisor who has a duty of care (banker, accountant, solicitor etc.).

The actions might be injunctions to stop fraud-related follow-up actions, insolvency proceedings, or freezing orders to prevent movement of defrauded funds or other assets. Many other actions are possible. A single fraud could give rise to several actions.

A word on GDPR

The new (from May 2018) General Data Protection Regulation (GDPR) exists to protect the digital rights and privacy of all European citizens. If your business has lost personal information as a result of fraud, you are legally obliged to report it. Fines for non-compliance are huge – up to €20m or 4% of global turnover (whichever is the greater). The National Cyber Security Centre (NCSC) offers plenty of guidance.

The Serious Fraud Office (SFO)

In case you were wondering, the SFO concentrates on investigating and prosecuting serious crimes involving financial wrongdoing, and complex economic crimes. It could be that what you witness in your own organisation is the thin end of a very large wedge. In which case, this is how the SFO approaches matters:

1. The SFO receives information on possible criminal activity.
2. A specialised team* considers the evidence and conducts its own research to assess the fraud's potential to become the subject of a criminal investigation.
3. The Director of the SFO considers the effect of the fraud on UK Plc, the financial sector in particular, whether there are reasonable grounds to suspect serious or complex fraud. This can lead to a case for criminal investigation.
4. If the evidence supports a realistic prospect of conviction and if a prosecution is considered to be in the public interest, charges will be normally be brought.
5. A court trial is usually time-consuming and complex. It usually involves masses of detailed evidence** and multiple defence advocates and witnesses.
6. The powers of the Proceeds of Crime Act 2002 and Criminal Finances Act 2017 can be invoked to recover the proceeds and reimburse the victims. This is further complex process in its own right.

It is possible for organisations to avoid a conviction by entering into a Deferred Prosecution Agreement. This involves a high degree of cooperation with the authorities and includes among other things, payment of compensation and penalties, and reimbursement of costs.

** The team comprises intelligence operatives, lawyers, accredited financial intelligence officers, analysts and investigators.*

***Crimes are increasingly global in nature, which is where Mutual Legal Assistance (MLA) comes in. It enables countries to request and provide help to each other.*

10. Conclusion

By now, you should be feeling optimistic about your ability to head off much external fraud before it causes harm. However, nothing is 100 percent certain, so you need to supplement the measures covered here with traditional audits and IT detection systems.

If fraud were a country, it would lie between Germany and Japan in GDP. (Based on Crowe's 2018 global fraud figure)

Fraud is the fastest growing crime and it is unlikely to slow down. It's already costing UK businesses over £100bn per annum, according to some reputable statistics as we have pointed out earlier in this report. Much of it can be avoided through practical common-sense and practical measures taken by the employees and management of your company.

Don't be a victim. Go on the attack!

GRAYDON
open in business

Graydon UK Ltd
2nd Floor Hygeia Building
66 College Road
Harrow, Middlesex
HA1 1BE

T: +44 (0)20 8515 1400
sales@graydon.co.uk

www.graydon.co.uk