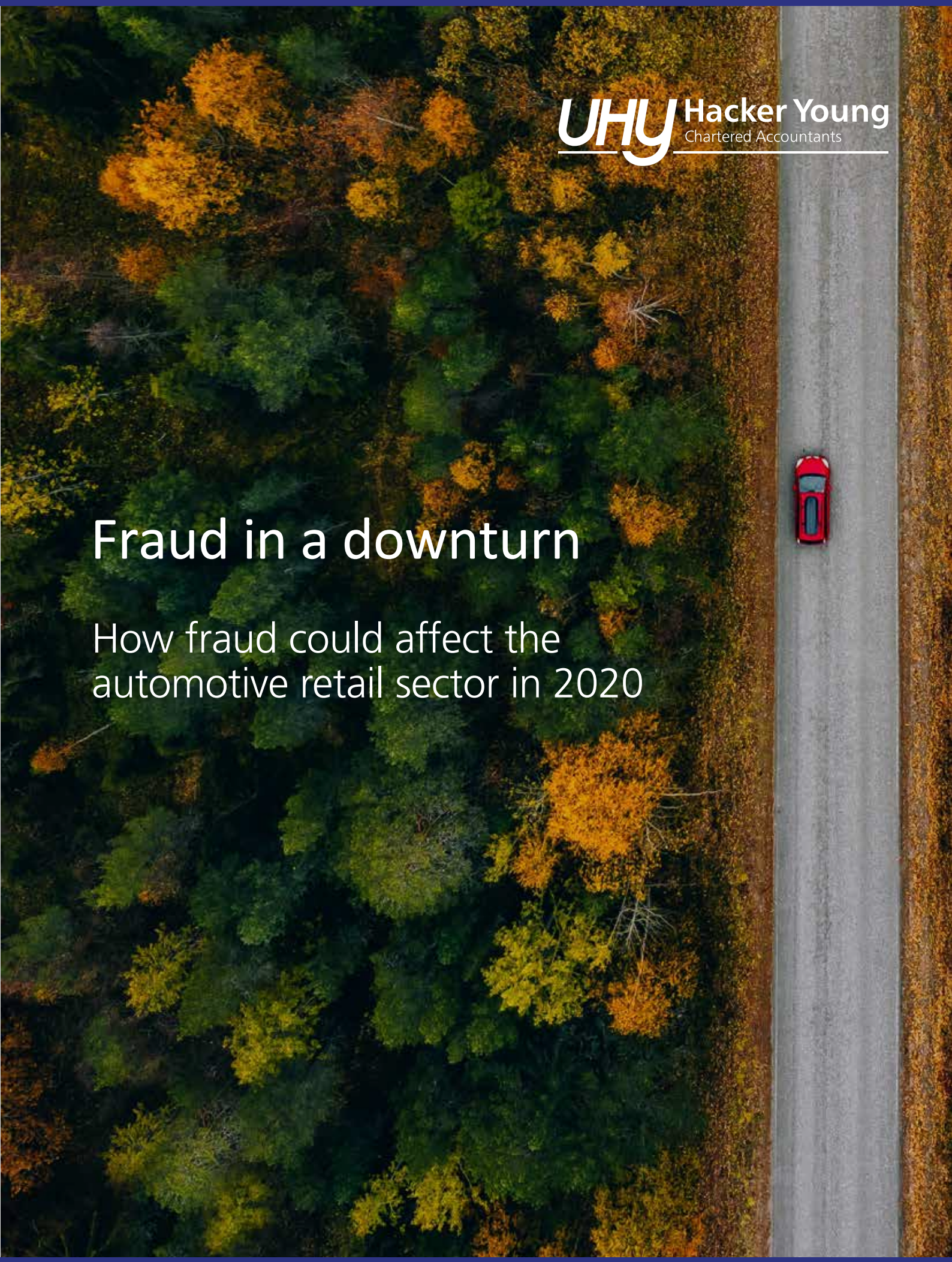


UHY Hacker Young
Chartered Accountants

Fraud in a downturn

How fraud could affect the automotive retail sector in 2020

www.uhy-uk.com/automotive

Helping you prosper

Fraud in the automotive industry

The events of the first half of 2020 represent one of the greatest challenges to business in the last 100 years and there is no doubt that the detrimental effect of the coronavirus pandemic on the UK economy will be substantial. The economic downturn that follows will result in many businesses and individuals struggling, with the prolonged disruption of COVID-19 likely to lead to a recession lasting a minimum of 12-18 months. As the economy declines, both in the UK and globally, new threats emerge and, in our experience, the occurrence of fraud is likely to increase.

When economic survival is threatened (either for an organisation or for an individual), the line separating acceptable and unacceptable behaviour can, for some, become blurred. In addition, fraud and other economic crime are increasingly becoming a focus of criminal activity and the government announced that fraudsters are exploiting the spread of coronavirus in order to carry out fraud and cybercrime. While some authorities are prepared to give leeway on certain risk mitigation activities, you need to ensure you remain alert to current and future risks.

Over the years, we have unearthed many different types of fraud, ranging from teaming and lading, back handers, profit manipulation and issues surrounding cash sales. You may wonder why, at your pre year-end audit planning meeting, your auditor queries whether there have been any instances of fraud during the year. It might seem a completely irrelevant question and one that has nothing to do with the audit but ask yourself, are your systems and controls robust enough to deter fraud? Would you know if your employees were pulling a fast one, or your supplier was really who they said they were?

The automotive sector has one of the highest percentage of frauds committed by insiders, so ensuring you have strong financial controls in place is essential. In April 2020, it was announced that Lookers was expanding its internal fraud investigations to its entire business after initial findings from one of its operating divisions resulted in an expected one-off charge of over £4 million in its 2019 financial results. By the end of June, the investigation had revealed a £19m issue in the accounts. This just illustrates how allegations of fraud, previously undetected, emerge from the shadows and can result in an eye watering black hole.

We have considerable experience dealing with common fraud risks and can work with you to help you protect the business. In this guide, we look in turn at the key types of automotive fraud, provide real case examples and consider strategies to manage risks.

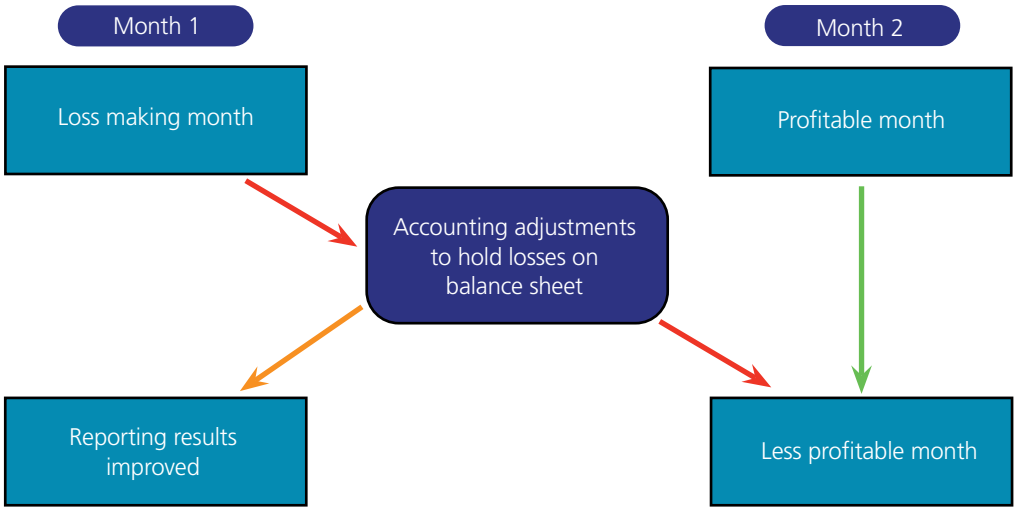

Helping you prosper

Profit manipulation

Not all fraud needs to be about cash. Sometimes, it can be about hiding the truth from more senior management, giving the impression that the results are not as bad as they really are.

What does profit manipulation look like?

In this example, a branch or a department has a poor month and know the results will be bad. Something important is riding on the results, such as a bonus or job security. The manager colludes with accounts to improve the results through an accounting entry; additional bonus income for example. The hope being that in the subsequent month, the loss can be released back when its impact is less visible.



To a lesser extent, the basics of this might be practiced every month, bringing forward sales to meet targets for example. The problem begins to escalate when the good month doesn't come round.

At this point, the fraud can begin to escalate with more and more being held on the balance sheet, which often is not subject to a rigorous review outside of the dealership team.

The balance sheet can often get past the auditors through clever or unverifiable explanations, or by creating enough confusion that a transaction cannot be successfully followed through.

The fraud is often perpetrated through the relative strength of the sales manager or dealer principal when compared to the accountant. The accountant is 'bullied' into the initial cover up on the promise that it will correct itself in the following month, when the results are much stronger. If this is not the case, then the manager is able to persuade the accountant that they are now fully implicated and so encourage further cover ups which compound the problem.

Solutions

Preventing fraud of this nature is by no means straightforward. However, there are a number of areas that can be considered, such as:

- Ensuring that the branch accountant has dual reporting lines into both local management and a senior member of the finance team
- Training the accounts team of the risks, and how such frauds are perpetrated
- Regular independent reviews of the balance sheet reconciliations, using internal or external resource. Particularly around known sensitive accounts that are easily manipulated such as vehicle bonus debtors
- Swap accountants between sites regularly, especially for holiday cover purposes
- In a group situation, ensure that very clear policies are in place with regards to the disciplinary consequences of any profit manipulation, no matter how small. For example, in one dealer group, it is an immediate sackable offence for the manager/accountant if such activity is discovered.

We have seen financial losses through profit manipulation build up into the £m's on balance sheets. Often the pressure is borne on the accounts team member rather than the manager who instigated the fraud. Any obvious pressure or stress exhibited by an accountant should prompt a cause for concern and a review of the balance sheet reconciliations instigated by a relevant internal or external party with the appropriate accountancy training.

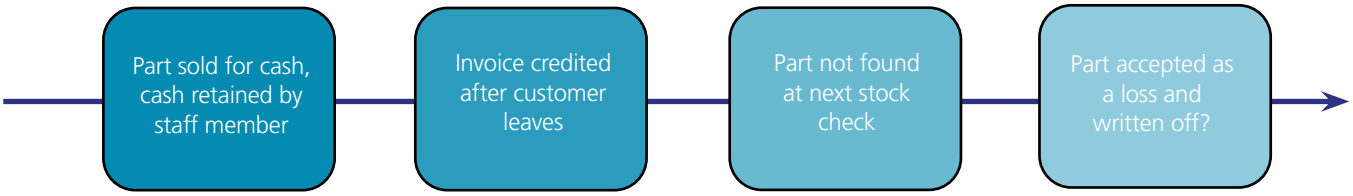
Cash and credit card sales

Members of staff are often trusted that they will give the cash on sale of an asset to the company; unfortunately sometimes this doesn't happen.

The basics

Cash sales are goods or services sold by a staff member who receives payment in cash or, in some cases, credit card.

An invoice is given to the customer and then credited, or only a proforma invoice given. The customer has their product and has paid for it, and the company's balance sheet does not show any debt is due. However, where a fraud has been committed, the cash has been retained by the employee or the employee's own credit card has been refunded.

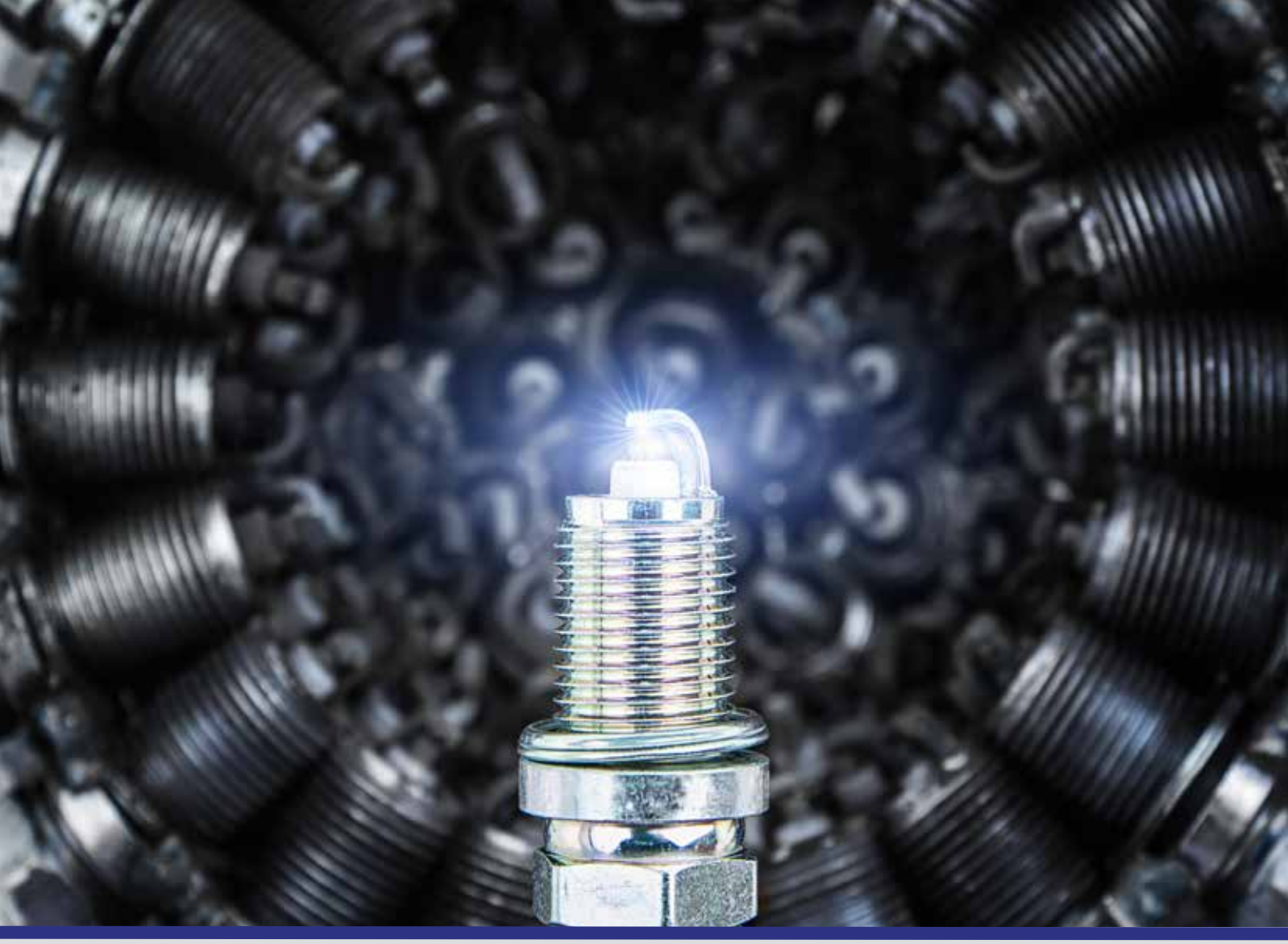


In the case of parts, the accounting is such that the credit note or proforma invoice means that the accounting records show that the part is still on the shelf. This will ultimately be picked up when a stock counting process takes place. However, the trail is not typically followed back to the perpetrator of the fraud. Instead, the parts stock will be found to be within tolerance overall and a write off processed in the accounts, effectively meaning that the fraudster has got away with it.

Real world example

We have seen an extreme example where the asset was a Range Rover that just became an aged stock problem as no regular stock check was performed. By the time the problem was discovered, the fraudster had moved on to another employer. More typically, the assets that are lost are parts and we have seen one case where one employee managed to remove £50k of sat nav systems.

Finally, it is still relatively common to see problems with obsolete parts, which are already provided for in the accounts (often written down to 1p on the system). It is, therefore, relatively easy for a parts person to set up their own eBay account and attempt to sell this stock for their own gain, in which case it can easily be invoiced off the system for the 1p cost.



Solutions

This type of fraud is difficult to detect if the fraudster is modest in their ambitions. Fortunately, this is rarely the case and a lack of detection emboldens the individual until eventually the scale of their fraud is detected.

There are, however, additional controls that can be implemented to prevent and assist with detection, including:

- Regular review of the credit notes that have been raised on the system, including monitoring volumes and value of credit note by individual to spot any unusual trends
- Perpetual stock counting procedures (many systems have controls to allow perpetual checking as part of normal daily routines)
- Detailed weekly review of overage parts and service WIP balances
- Reviewing PDQ credits for volume and value.

Naturally, it also makes sense to discourage the use of physical cash with the customer base wherever possible.

Teaming and lading

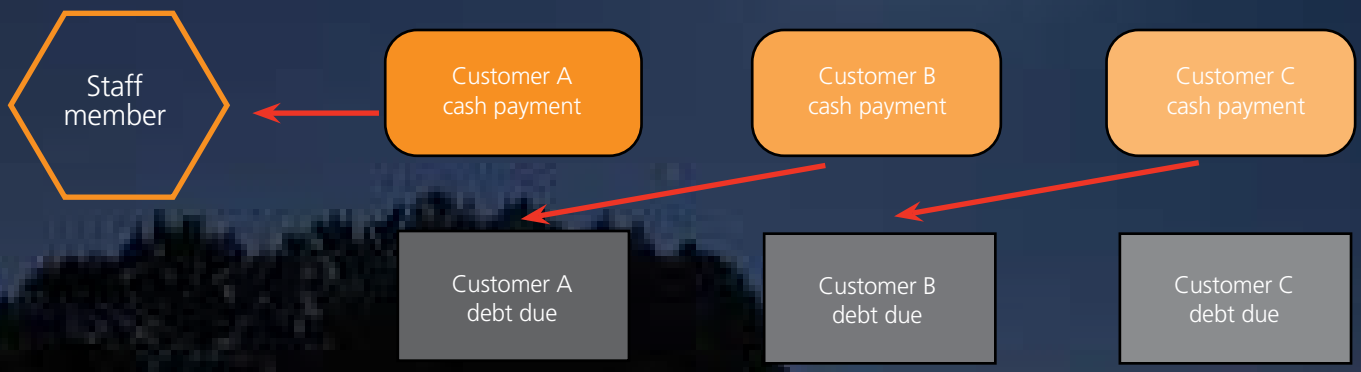
Teaming and lading is one of the most common types of fraud and will often start with just a small amount of money. If the fraudster finds that they get away with 'borrowing' the money, the amounts will escalate.

Teaming and lading can either be a cash fraud or a way of covering over errors.

If a cash fraud, it can be perpetrated by any staff member with access to cash, so sales staff taking deposits as well as service and part advisors who can take cash.

The basics

A member of staff receives cash which they keep for themselves. A debt is left due in the company's balance sheet. A subsequent cash receipt is allocated to the original debt and in this way an over age debt may never become apparent.



An example we observed saw a sales person keep a deposit from a customer and use this to feed a gambling habit. As the sales person was able to make excuses, the fraud went undetected for several months and the amount taken began to increase. Eventually, the sales manager was challenged on the size of the debt outstanding and the fraud was uncovered.

The sales person had no assets and so nothing could be recovered.

This type of fraud can also be used to cover over errors which can be even more costly for a business. One of the typical errors we see occurs when a dealer has poor processes over vehicles transferred to another dealer; so the vehicle is transferred, but the manufacturer debits the originating dealer in error. This error should be picked up in regular monthly manufacturer reconciliations, if properly performed.

Real world example

In one of the biggest examples we have seen, a branch accountant was struggling with their workload but didn't want to ask for help. There was a lack of regular reconciliation of the ledger balance to the manufacturer statement, and no review procedure in place. The branch accountant was afraid of admitting that they had not been doing their job properly and so, to avoid the ageing looking odd, the oldest invoices were matched against any similar payment. Eventually the payments outweighed the invoices, but this could be explained as simply timing differences. It was only on a change of auditors to a motor trade specialist (who insisted that the account was properly reconciled) that the error was discovered. The business needed to provide over £500k in its accounts, although over a number of years they eventually managed to identify some of the amounts and recover them from the other dealers who were wondering how they had received the vehicle for free.

Solutions

Most solutions rely on strong initial controls, rather than means of detection, through policies such as:

- Strong segregation of duties between the person receiving the cash and the person posting it onto the system
- Full reconciliations of all balance sheet accounts on a monthly basis, with a review of those reconciliations being carried out by appropriately qualified member of the management team
- For larger businesses, the use of an internal audit function to provide some independent verification
- Insisting on key personnel taking their holidays (these types of fraud quickly unravel when somebody else is tasked with running the ledgers in their absence).

In addition, management need to be aware of lifestyle changes and rumours amongst the team which would drive the temptation to defraud. We have seen various examples, including expensive clothes, holidays, rumours of gambling or drug addiction, marital problems etc.

Kick back/back handers

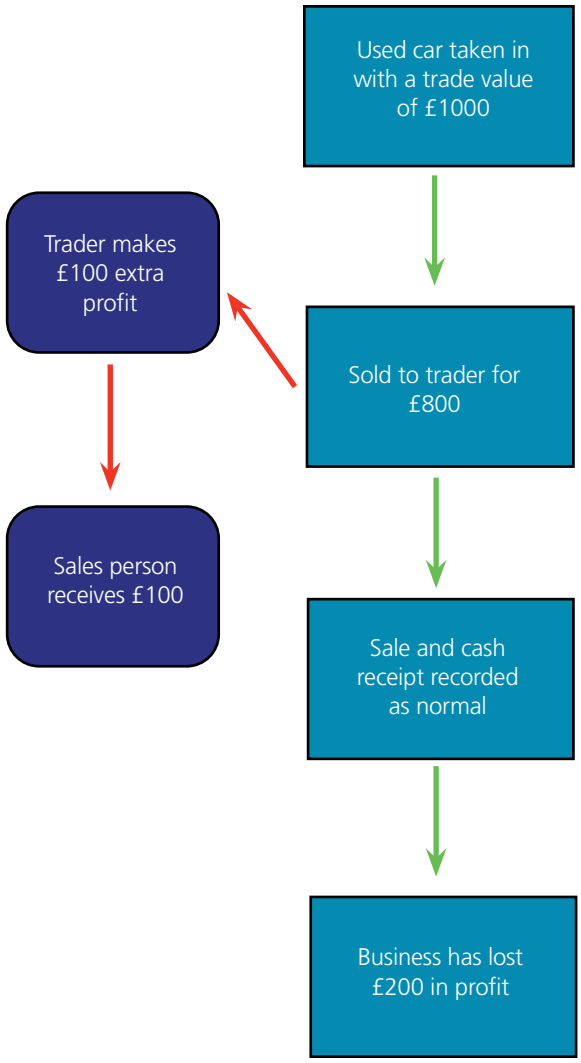
One of the hardest frauds to identify, this is where an employee is being paid by a supplier or customer to source or give them business.

The sales and purchases still take place and are recorded and paid for in the usual way. The impact being that the price paid for goods may be high compared to a competitive quote, or sales price achieved too low. The business, therefore, loses out through reduced profit.

Real world example

The most widely known example of this type of fraud is when part exchange cars are sold onto traders. A sales manager we recently met experienced this on his first day at a new job, when a trader approached with the offer of cash in exchange for a lower price or guaranteed business.

Such a fraud is equally possible with suppliers offering payments to secure a sale.



Solutions

We still hear of instances where owners accept that such practices are part of the 'normal' motor trade practice and that this will always happen to some extent. However, if you take the view, as we do, that this is not acceptable, then typical safeguards include:

- Auction only policies for trade vehicles or, in an owner managed business, the trader relationship remains with the owner.
- Fixed/group policies or suppliers in place for sensitive areas of supply including:
  - Auction fees
  - Valeting fees
  - Sub contract fees (smart repair etc)
  - Local advertising/marketing
  - Recruitment fees
  - Cleaning contracts
  - Security contracts
- Detailed analysis and comparison of the cost base/metrics across the group (or using third parties) to identify and investigate cost variances from site to site.

Supplier fraud

This particular fraud occurs when weaknesses within the financial control process present an opportunity for a fraudster to extract cash from the business via the initiation of unauthorised payments or via the creation of a legitimate expectation of payment based on fraudulent invoices. This type of fraud can have a devastating impact as it is generally undertaken by determined, informed and methodical individuals over a protracted period of time, ultimately depriving the business of cash whilst the management struggle to comprehend reasons for such lack of cash availability.

Generally, financial systems and controls tend to reflect the size and nature of a company. The occurrence of this type of fraud is, therefore, more notable in smaller entities where control processes are reliant on a limited number of individuals or in larger businesses where the sophistication of a control process does not match the size of the company, or where key mitigation controls are implemented sporadically, if at all.

Real world example 1

A legitimate purchase order is placed into the system for a product which is purchased on a regular basis and, generally, a good level of stock is maintained. In this instance, the order is for a lower quantity of stock. Next the purchase order is duplicated on the system under the pretence that this is making good an error made in the prior order, to ensure that the expected level of stock is ordered.

On receipt of the products associated with the first order, the goods received documentation along with the subsequent purchase invoice are entered into the system. These are then also duplicated with fraudulent reference numbers and re-entered on to the system.

This action has created an expectation of payment within the system and the fraudster waits until the terms associated with this invoice mandate settlement. On the date of settlement, the first invoice is included into a payment run of legitimate invoices and the process is completed. However, following this payment, the fraudster's bank details are entered into the system in place of those of the supplier and the fraudster now seeks approval for settlement of the fraudulent invoice. Usually authority for this payment is sought from an individual who would not normally authorise payments, but is there as back-up, with the pretence being maintained by the fraudster that the purchase invoice was missed off the last run.

On completion of the bank payment, the fraudster returns the bank details to those of the supplier. Having settled the liability, the supplier account is up to date and the bank will appropriately reconcile on review.

If effectively spread across inventory, this type of fraud can go unnoticed for many months. In this particular instance, the fraud was exposed when the Finance Manager went on holiday and his assistant spotted paperwork on his desk that other team members would ordinarily deal with. It was discovered that, as a default, the Finance Manager had the ability to undertake any number of duties within the finance system and controls as a means of back up for other team members. This enabled the individual to maintain a pretence that in these limited instances he was helping out other team members; and in the process extracted nearly £80,000 in cash.

Real world example 2

This example highlights the use of teaming and lading within a purchase ledger. A Finance Manager of a small finance team has involvement in many aspects of the financial control function but cannot authorise payments above £1,000, does not authorise payment schedules, and does not review trade creditor or bank reconciliations. Critically, this individual has become aware that that certain key mitigation controls are not effectively undertaken by the Finance Director, if at all, due to a trust built up within the team. The Finance Manager's personal circumstances change.

The Finance Manager sets up a payment schedule for a range of trade creditors due for settlement but selects a number of invoices as being in dispute, totalling up to less than £1,000. This payment schedule is authorised by the Finance Director. The Finance Manager writes themselves a cheque for the value of the disputed invoices, processing both the original payment run and the cheque as having cleared all the trade creditors due for settlement that month.

The supplier begins to chase for the unpaid invoices and the Finance Manager assures them that settlement is forthcoming. The Finance Manager explains to the Finance Director that purchase credit notes were received from the supplier, explaining why there is no longer any sums due to these suppliers.

The following month, the Finance Manager prepares a payment schedule that seemingly clears the current month's trade creditors, but incorporated within the schedule is the settlement of the prior month's unpaid invoices. Once this payment schedule is processed, the disputed supplier invoices have now been refreshed to incorporate current invoices.

Unlike Example 1, the Finance Manager is left exposed to the extent that the cash extracted from the business now represents the amount of supplier invoices being treated as disputed in any one month. However, such sums can be immaterial when compared to the size of outstanding trade creditor balances in any one month. In this instance, the Finance Manager had managed to extract £25,000 from the company over a period of six months. The fraud was only exposed when a supplier chasing unpaid invoices happened to get through to the Finance Director as the Finance Manager was not first in the office due to unforeseen circumstances.

Solutions

This type of fraud is difficult to detect if the fraudster is modest in their ambitions. Detection in the absence of a wholesale review of the company's financial control processes tends to result from a mistake being made by the fraudster.

Primarily, this fraud is mitigated by robust system and control processes. It is recommended that any control should, as a minimum, adopt a suitable level of segregation of responsibilities. For example, individuals able to set up a bank transaction should not be the same individuals responsible for approving and/or authorising these transactions. In the case of a purchase, the individual placing a purchase order should ideally not be the same individual who would check the goods into inventory, process the purchase invoice or set up the supplier on the system in the first instance.

Where there are limited resources, as a minimum implement segregation at the critical authorisation points in a process and increase senior management key control reviews on areas such as bank reconciliation, purchase ledger control account reconciliation, variance analysis in management accounts and aged profile of trade creditors.

Additionally, management should be mindful of individuals within the finance team whom demonstrate any of the following:

- Not taking holidays
- Consistently first in and last to leave
- Working long hours beyond those deemed necessary to role
- Personal lifestyle seemingly disproportionate to salary
- Unnaturally protective of their personal work space
- Intimate relationships with colleagues within the immediate control process – providing the fraudster an ability to coerce others and circumvent segregation of duties
- Covering processes for other team members whether due to failure to fill a role, maternity or other long term absence – the time provides the opportunity to initiate the modest extraction of cash.


Helping you prosper

Cybercrime

According to a recent government survey, almost half of businesses (46%) report having cyber security breaches or attacks in the last 12 months. Whilst cybercrime is the most common type of reported fraud, prevention can be difficult.

Cyber extortion

Cyber extortion is an online crime where hackers break into your systems and hold your data, website, computer systems, or other sensitive information hostage until you meet their demands for payment.

Ransomware is used to infect computer systems, with a virus encrypting every data file it finds and displaying a ransom note to the user. The extortion message usually starts by demanding an online payment of anywhere from hundreds to thousands of pounds in return for the decryption keys needed to restore the locked files. The demand often includes a series of deadlines for payment; each missed deadline leads to a higher ransom demand and perhaps some destroyed files. If you do not pay up, the attacker discards the decryption keys, making the data permanently inaccessible.

Email impersonation

Email impersonation is becoming increasingly common and increasingly sophisticated. Plausible emails, often purporting to be from the CEO or Financial Director, ask for an amount to be transferred to a bank account. These often cleverly mention where a person is (eg. a conference or meeting), after the fraudster has hacked into the system and checked their diary. Where the fraud is successful, sums are transferred without telephoning the individual to check the request is genuine. The same process is used in emails allegedly coming from a supplier or employee, advising that their bank details have changed. If the accounts department does not check directly with the supplier or employee, future BACS payments are then diverted into a fraudsters' account.

Solutions

Cybercrime is ever evolving and staff need to be encouraged to be sceptical about everything. From a parts supplier informing you of new bank details, to an email from the dealer principal requesting the immediate transfer of funds, to a call from the bank to say there is a problem with the payment run. Your accounting systems must have strong controls in place which include double-checking instructions before transferring funds or changing bank details.

To help protect your business from cybercrime, ensure you:

- Have robust IT systems and up to date software
- Have comprehensive business interruption insurance in place that will protect you if you are victim to a cyber extortion or other types of cybercrime
- Comply with General Data Protection Regulation (GDPR) rules to protect data
- Hold regular awareness training for staff to help them detect suspicious behaviour
- Do not open emails from unknown sources, and be suspicious of poor spelling
- Are extremely wary of urgent email requests for any personal or financial information
- Call the company or individual in question with the number listed on their corporate website. Avoid using phone numbers within the email, as they could be fake
- Do not divulge personal or financial information via the internet unless the site is secure
- Do not use the links included in the email unless you are certain that the email is legitimate.

Cyber liability insurance is often not fully understood in terms of what it covers and how it will respond in potentially harmful situations. We recommend that you speak to your insurers to make sure you have a good understanding of how you are covered.

Protecting your business

COVID-19 has far reaching implications, the extent of which are still becoming apparent. However, history suggests we should expect to see a wave of fraud and other economic crime arising from this period in the months and years to come.

You should therefore be taking steps now to ensure you are best placed to prevent crime from occurring and have systems in place to deal with it in the event that it does occur.

To reduce the risk of misconduct, you should review financial controls and put measures in place to ensure the continuation of a strong control environment. In addition to the specific solutions outlined above, as a minimum we recommend you:

- Review the strength of financial controls and internal processes and guidelines
- Remind employees of existing company policies governing conduct and the acceptable use of company systems, devices and information
- Put measures in place to identify any unusual behaviour, such as enhanced monitoring or retrospective review of high-risk transactions
- Warn employees that cyber criminals may exploit the current turmoil to increase phishing attacks
- Review cyber liability insurance and understand how it will respond in potentially harmful situations
- Discuss automotive retail fraud risks with your auditor during the audit planning meeting to ensure key risks are identified and responded to.

Need help?

Fraud and accidental error is a major risk for the automotive retail sector. We have outlined only a few examples of the risks faced by motor dealers on a day to day basis. The key message is to remain vigilant and implement robust systems and controls that are regularly policed and enhanced where appropriate.

If you would like to discuss fraud in more detail or find out about how we can help you develop strong financial controls, please contact us to discuss your specific circumstances.

David Kendrick
Partner

e: d.kendrick@uhy-uk.com
t: +44 161 236 6936

Paul Daly
Partner

e: p.daly@uhy-uk.com
t: +44 161 236 6936