

Protect your shipment*

Supporting Transportation & Logistics companies in managing fraud risks



*connectedthinking

PRICEWATERHOUSECOOPERS 

PricewaterhouseCoopers actively partners with industry to combat fraud and misconduct. This report draws upon several other PricewaterhouseCoopers publications including [Predicting the unpredictable: Protecting Transportation & Logistics companies against fraud, reputation and misconduct risk](#) and [Key Elements of Antifraud Programs and Controls: A White Paper](#). We also include an industry-specific summary of the results of the [Global Economic Crime Survey 2005](#) in the appendix, to help companies understand the magnitude of the problem.

Key contacts

Global Transportation & Logistics Industry Leader

Klaus-Dieter Ruske
+49 211 981 2877
klaus-dieter.ruske@de.pwc.com

European Transportation & Logistics Industry Leader

Andreas Baur
+41 58 792 53 56
andreas.baur@ch.pwc.com

UK Transportation & Logistics Industry Leader

Clive Hinds
+44 1727 89 2379
clive.p.hinds@uk.pwc.com

Global Transportation & Logistics Business Development

Peter Kauschke
+49 211 981 2167
peter.kauschke@de.pwc.com

Global Investigations & Forensics Leader

Steven Skalak
+1 646 471 5950
steven.skalak@us.pwc.com

Lead Partner, Global Economic Crime Survey

Claudia Nestler
+49 69 9585 5552
claudia.nestler@de.pwc.com

US Fraud Risks & Controls Practice Leader

Jonny Frank
+1 646 471 8590
jonny.frank@us.pwc.com

For additional contacts in your country, please see the Contact Us page at the end of this report.

PricewaterhouseCoopers provides industry-focused assurance, tax and advisory services for public and private clients. More than 140,000 people in 149 countries connect their thinking, expertise and solutions to build public trust and enhance value for clients and their stakeholders. Our Transportation & Logistics practice is a global network of partners and client service professionals dedicated to postal, express and logistics service providers, airlines, shipping companies and transport infrastructure operators.

© 2006 PricewaterhouseCoopers. All rights reserved. PricewaterhouseCoopers refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity.

*connectedthinking is a trademark of PricewaterhouseCoopers LLP.

Contents

- 5 Fraud does happen –
and not just at other companies
- 6 Fraud schemes in
Transportation & Logistics
- 10 Mitigating the threat – how to take
action against fraud
- 15 Appendix – results of the
Global Economic Crime Survey
2005
- 19 PricewaterhouseCoopers
global Transportation & Logistics
contacts



Fraud does happen – and not just at other companies

Fraud isn't always a non-violent crime – in 1977 the world was rocked by the sinking of the ship “Lucona” in the Pacific ocean after an explosion, with six people losing their lives. The ship's owner claimed 20 million US dollars from his insurance policy, asserting that the ship was loaded with expensive uranium tilling machines. In reality the cargo was worthless; a fact which only came to light after attempts at obstruction by several politicians who were close friends of the owner. The Austrian Minister of Defence, a shareholder in the firm involved, committed suicide after it came to light that he had given permission to deliver explosives to sabotage the ship.

Fraud has continued making headlines into the 21st century, with recent examples in the nineties being scarcely less explosive than the sinking of the Lucona, yet many executives still believe that “fraud can't happen in my company”. But fraud does happen, and often – nearly half (45%) of organisations in the Transportation & Logistics industry¹ report have experienced fraud over the past two years, and the actual incidence of fraud may be even higher, as detection can be difficult.

45% of Transportation & Logistics companies surveyed have experienced fraud over the past two years.

While the cost of fraud is not often counted in human lives, it can nonetheless be very damaging; direct financial costs can be substantial. Indeed, one-fifth of executives reported that they viewed the financial impact of the two most serious incidents of economic crime at their companies as being very serious.² Furthermore, fraud can damage a company's competitive advantage, employee moral, and vendor/supplier relationships. Attention is often focused on financial statement manipulation and other forms of financial misrepresentation as well as corruption and bribery. However, fraud and economic crime is a broader issue that poses risks to all aspects of a company's operations, and can also impact reputation and strategy.

One-fifth of executives view the financial impact of the two most serious incidents of economic crime at their companies as being very serious.

Governments in all parts of the globe have developed legislation designed to fight economic crime. Companies must navigate the regulatory minefield not only in their home territory, but also in every country in which they are operating.

This report will outline some of the most common fraud schemes in the Transportation & Logistics industry and provide suggestions on combating fraud. Where relevant we have also incorporated industry-specific insights from the results of our *Global Economic Crime Survey 2005*; a summary of results for companies operating in the Transportation & Logistics industry is included in the appendix. For more extensive information on developing an anti-fraud programme and specific guidelines for SEC-listed companies, please see our recent publication, *Predicting the unpredictable: Protecting Transportation & Logistics companies against fraud, reputation and misconduct risk*³.

What is fraud?

We use the term fraud to denote wrongful or criminal activities to or in an organisation, intended to result in the gain of money or benefits for the perpetrator(s).

¹ This figure is taken from results of PricewaterhouseCoopers' *Global Economic Crime Survey 2005*. Overall results of the survey are available at www.pwc.com/crimesurvey; a summary of results for companies operating in the Transportation & Logistics industry is included in the appendix.

² Ibid.

³ Available at www.pwc.com/transport

Fraud schemes in Transportation & Logistics

Did the goods arrive?

Cargo theft and other types of asset misappropriation

The average layperson, when asked to describe fraud, will probably think of fairly straightforward examples of the **misappropriation of assets** involving theft. Certainly this type of fraud does happen fairly frequently in the Transportation & Logistics industry; particularly cargo theft. Cargo theft occurs in a range of freight-forwarding and storage operations, but the greatest risk is during truck and container transportation or when vehicles are in the process of being loaded or unloaded. The trend towards extensive subcontracting and use of owner drivers has increased the risk of cargo theft in the trucking industry; the now widespread use of sealed containers and “track and trace” systems has helped to reduce petty pilferage but allows for large-scale cargo theft.

Asset misappropriation in general is by far the most prevalent type of fraud in the Transportation & Logistics industry, with 73% of companies who report having experienced fraud naming this type. In addition to cargo theft, the term also covers a wide variety of other methods of diverting assets to private use.

Leaking money

Inadequate controls can lead to revenue leakage

Transportation & Logistics is a dynamic, changing industry – many companies are entering new markets and making acquisitions. While growth in general is good for the industry, it also poses challenges to control systems which may not yet be keeping up with the new status quo – thus opening the door to potential fraud.

One example – when a company’s systems do not yet link shipping, billing, and revenue recognition functions for all subsidiaries, opportunities arise for revenue leakage.

Revenue leakage occurs when there are discrepancies between the quantity of items shipped, and the quantity of items for which revenue is being recognised. This is a very important issue for the transportation industry because, in many cases, companies ship thousands of items per day. This scheme can also occur when a transportation move involves inter-company handoffs.

Cooking the books

Narrow margins increase temptation to manipulate financial statements

Opportunity is not the only factor that drives perpetrators to commit fraud; motive also needs to be present. Most segments of the Transportation & Logistics industry are operating within very narrow margins, a situation which can lead to enormous pressure on management to achieve revenue and profit targets, and thus generate the motive for **financial statement manipulation** which may help achieve these goals. This type of fraud sometimes happens via another aspect of revenue recognition which provides opportunities for fraud – timing estimates, i.e., the manual adjustments made to the financials to record revenue. Most accounting standards provide that revenue and direct costs may be recognised when the shipment is completed, or alternatively revenues can be allocated between reporting periods based on relative transit times in each reporting period with expenses recognised as incurred. In some cases, management must use estimates and judgement to adjust the amount of revenue recognised. As a result, there is the potential for management to manipulate the estimate to over- or understate the amount of revenue or cost recognised in a period.

Who hired this guy anyway?

Decentralised structures may lead to fraudulent disbursements

The Transportation & Logistics industry is generally very decentralised; airlines may have ticketing offices and ground personnel in numerous locations and countries around the world, railways likewise have ticketing and other agents in many different locations, shipping companies have many delivery hubs and drivers. This type of structure can pave the way for **fraudulent disbursements**.

Fraudulent disbursements comprise a wide range of fraud schemes which result in cash being inappropriately sent from the company to another party. Examples of fraudulent disbursement schemes include payments to ghost employees, fictitious vendors, pay-and-return schemes, over-billing schemes, unauthorised overtime schemes, and expense report schemes.

The right hand knows what the left hand is doing – counting the cash!

Failure to segregate cash receipt and cash application duties can lead to cash skimming.

Decentralisation can also lead to **cash skimming**. Cash skimming is often a result of a lack of segregation of duties in the areas of cash receipt and cash application. Common schemes include not recording payments received against the customer's account and then writing off receivable balances left unpaid. In the Transportation & Logistics industry such schemes can sometimes go undiscovered over long periods of time, as new payments can obscure the missing balances. Indeed, this type of fraud has led to crippling damages and even bankruptcy for a few Transportation & Logistics companies in recent years.

A less elaborate variant in the Transportation & Logistics industry involves delivery personnel accepting cash-on-delivery (COD) payments and failing to record them.

Show me the money

Commercial bribery and kickbacks may also be a risk

Commercial bribery, in the Transportation & Logistics industry, may also be a significant risk as a result of decentralised operations. Commercial bribery can involve any step along the supply and sales chains and take many forms, including kickbacks to procurement departments or vendors, slotting fees, etc. Given that all the involved parties are seeking to cover up their activities, it can often be difficult to uncover such schemes, which may develop an extensive network that goes undiscovered for an average of 3–6 years.

Further, once an employee has participated in this type of corruption, he or she becomes vulnerable to blackmail by confederates and may find it impossible to cease making the illegal payments.

Taking the tax authorities for a ride

Carousel frauds make use of opportunities for falsification in cross-border shipping

Most segments of the Transportation & Logistics industry are operating in numerous countries around the world. The “value-added-tax (VAT) merry-go-round” style of fraud scheme (also referred to as a carousel fraud) takes advantage of the opportunities for falsification which arise when goods are shipped across borders. In this kind of **tax fraud**, a shipment of goods is falsely documented as crossing several national borders. As the “goods” move on to the next country, VAT is re-claimed and pocketed. Eventually the non-existent goods arrive at a dummy company or bankrupt entity and the trail ends.

This scheme is essentially a sophisticated variation on recording fictitious transactions, the creating of fictitious orders for either existing or fictitious customers.

Tricking the trucker

Transportation & Logistics service providers can find themselves liable for VAT, import duties, excise, and even penalties on shipments

Many Transportation and Logistics companies provide services around the application of customs and excise procedures and customs clearance. This situation can lead to companies being defrauded by their customers, as the service provider itself may be **partly or fully liable** for import duties and, where applicable, excise and VAT at import that could become due.

In some instances, the service provider is supplied with incorrect information on the goods, clears the goods on the basis of that information and at a later audit of Customs will be responsible for the understatement of the duties. As the actual control on the clearance often happens retrospectively, the principal may have disappeared in the interim. Goods may also be brought or shipped under a suspensive customs regime (i.e. the duties due are not paid) for which the service provider is liable. The principal then “arranges” the removal of the goods from this procedure without fulfilling the proper clearance procedures, resulting in the service provider being liable for the payment of the import duties, excise and, where applicable, VAT at import (not deductible for the service provider) and potentially, penalties.



The man with the golden laptop

Industrial espionage can threaten chances of winning major contracts

Major contracts are the bread and butter of many Transportation & Logistics companies. Exclusive agreements to provide delivery services or priority status as an airline or rail provider for a major company can make a much more substantial difference to the bottom line than individual packages or travel arrangements. Advance information about a competitor's pricing structure can help to win major contracts such as a framework delivery agreement, making industrial espionage potentially lucrative.

Recent new technologies such as cell phone and PDA cameras have made it easier to copy sensitive documents, and ultra-sensitive microphones can help perpetrators listen in on confidential meetings. All too often this type of industrial espionage is perpetrated by company insiders. In addition, many company networks remain vulnerable to the activities of hackers, who may be involved in industrial espionage.

Greasing government's palm

Major capital expenditures may increase the likelihood of bribery of public officials

The size and scope of capital expenditure projects such as airline terminal construction and railroad infrastructure expansion make the transportation industry particularly susceptible to bribery. Many of these types of major projects may lend themselves to fraud involving using inaccurate statistics and estimates to gain government subsidies. As subsidies often come from different governmental entities (for example, EU, federal government, state government), there may be little incentive to track down and appropriately punish offenders.

In addition, transportation companies often do not have mature Foreign Corrupt Practices Act (or local bribery legislation) compliance programmes as in the case in some other sectors, such as defence contracting and health care.

On-time or else

Contingency services may not be documented and provide the potential for abuse

Delivery services operate in an extremely fast-paced environment, where packages often must be delivered on-time or risk serious penalties. In order to meet deadlines, local delivery hubs may have to arrange for contingency services such as couriers to perform the last leg of the service, or rent vehicles to replace delivery trucks which are under maintenance. These contingency services may be quite costly, and are not always documented – they thus represent another area which is rife for abuse by enterprising fraudsters.

Managers may also be tempted to accept kick-backs from such operators, so this is another area which should be monitored for possible instances of commercial bribery.

Mitigating the threat – how to take action against fraud

Believing that your company will never be subject to fraud can be a vicious circle – if you don't look for fraud, you probably won't find it, and if you don't find fraud, you may assume it's not there and not set up systems to detect it. Transportation & Logistics executives need to break this cycle and take appropriate action to protect their companies from fraud. By fostering a culture of honesty and high ethics, evaluating and improving anti-fraud processes and controls, and developing an appropriate oversight process, executives can reduce the risk of serious fraud and alleviate the consequences of fraud if and when it happens.⁴

The right people with the right attitude will make the right choices

Corporate culture begins at the top. That's why it's critical that executives set the tone and display exemplary standard of honest and ethics in dealing with their employees. It's also important to see that fraud gets, and stays, on the agenda in board meetings and other top-level communication venues. Establishing a consistent control environment should be one of management's top priorities. The control environment refers to such intangibles as integrity, ethical values and competence of the entity's people, and management's philosophy and operating style, but it also covers more concrete expressions of these intangibles, such as the way management assigns authority and responsibility, and organises and develops its people. In addition, the control environment sets out the role of the audit committee and board of directors. The control environment has pervasive influence on the way business activities are structured, objectives are established and risks assessed. It also influences control activities, information and communication systems and monitoring activities. The control environment is not static; it is influenced by the entity's history and culture and in turn influences the "control consciousness" of its people in performing their day-to-day activities.

Establishing a sound control environment is key to managing fraud risk.

An effective code of conduct is a fundamental element of an effective control environment and antifraud program. The code should outline clear and objective standards for compliance and set up a fair process to determine viola-

tions. It should include all employees to ensure that any observed instances of misconduct or pressure to compromise ethics standards are reported.

The code of conduct also must be communicated effectively (through the employee handbook, policy manual, intranet, etc.) on a periodic basis to all covered persons. Ineffective communication prevents even a comprehensive code of conduct from being effective and contributing to an appropriate "tone at the top".

Employees should evidence their receipt and reading of the code. This is generally accomplished through a confirmation process. Annual confirmations from the covered persons regarding their compliance (or lack thereof) with the code of conduct, including appropriate follow-up regarding lack of response and any exceptions noted, are recommended.

Requiring attendance at training at the time of hiring and periodically thereafter evidences the entity's commitment to ensuring that the employees understand the code. Training should address the "tone at the top", code of conduct, and the individual's duty to communicate or report actual or suspected fraud or misconduct. Interactive training may provide evidence that a code has been communicated, and that employees have received, read and understood the code.

Motivated and satisfied employees are not only more productive, they are also less likely to commit fraud. Creating a positive workplace environment is therefore a key component to deterring fraud, as is instigating suitable procedures for hiring and promoting appropriate employees. Establishing standards for hiring and promoting the most qualified individuals, with emphasis on educational background, prior work experience, past accomplishments and evidence of integrity and ethical behaviour, demonstrate an entity's commitment to competent and trustworthy people. Such standards should include the performance of background investigations on individuals being considered for employment or for promotion to positions of trust within an organisation.

A company's commitment to fostering high ethical standards within its workforce doesn't end once an employee's contract is signed. To the contrary, companies need to train employees and develop mechanisms for on-going communications, training and confirmation, as already noted in reference to the code of conduct.

⁴ For more information on mitigating the threat of fraud, please see our publication [Key Elements of Antifraud Programs and Controls: A White Paper](#).

Appropriate response to incidents, including in-house communication of relevant consequences, can also play an important role in ensuring that a suitable level of discipline in preventing fraud is achieved within an organisation.

Whistleblowing systems can support an effective code of conduct and are an important part of establishing open and effective communication within an organisation. These systems should be seen as a supporting mechanism to help discover fraud rather than as a sign of mistrust. While companies should discourage employees from giving anonymous tips, it's important to ensure that this avenue remains open. Companies should also establish a system of validating tips to avoid accusing employees of corruption without adequate grounds.

Assessing the threat

Organisations should consider the potential for fraud as part of their enterprise-wide risk assessment process or risk management program. Fraud risk assessment expands upon traditional risk assessment. It is scheme and scenario based rather than based on control risk or inherent risk. The assessment considers the various ways that fraud and misconduct can occur by and against the company, including an assessment of which processes are more susceptible to fraud and the level of difficulty of accomplishing the fraudulent activity (e.g., does it require an inside or outside collaborator, special knowledge, etc.).

Fraud risk assessment also considers vulnerability to management override and potential schemes to circumvent existing control activities, which may require additional compensating control activities. The fraud risk assessment process should consider the extent of vulnerability of the entity to fraud and its potential impact. A comprehensive assessment of fraud risk should include the potential for fraudulent financial reporting, misappropriation of assets, and unauthorised or improper receipts and expenditures. The risk of fraud by senior management or the board should not be overlooked, particularly as management-level fraud can be the most damaging to an organisation.

To be effective, management should perform fraud risk assessments on a comprehensive and recurring basis rather than in an informal or haphazard manner. Risk assessments should also occur when special circumstances arise, such as changed operating environments, new products and markets, and corporate restructurings. Management should include fraud risk in these assessments.

Management must also assess fraud risk at the company-wide, business unit and significant account levels. The nature and extent of management's risk assessment activities should be commensurate with the size of the entity and complexity of its operations (for example, the risk assessment process is likely to be less formal and less structured in smaller, centralised entities).

Once executives have a comprehensive understanding of the fraud risk present at their companies, the organisation should identify the control activities implemented to mitigate the identified fraud risk. In the context of an antifraud management program, control activities are those actions taken by management to identify, prevent and mitigate fraudulent financial reporting or misuse of an organisation's assets. Antifraud control activities should occur throughout the organisation, at all levels and in all functions. They include a range of activities as diverse as approvals, authorisations, verifications, reconciliations, segregation of duties, reviews of operating performance and security of assets.

Taking steps to mitigate risks is critical, such as segregation of duties, reviews of operating performance, or simply approval systems.

Management should evaluate whether appropriate internal controls have been implemented in any areas identified as posing a higher risk of fraudulent activity (such as revenue recognition and non-standard journal entries), as well as controls over the entity's financial reporting process and the potential for management override. Because of the importance of information technology in supporting operations and the processing of transactions, management also needs to implement and maintain appropriate controls, whether automated or manual, over computer-generated information.

The environment in which an entity operates affects the fraud risks to which it is exposed and may present unique external reporting requirements, or special legal or regulatory requirements. An entity's antifraud program must consider whether the controls implemented are adequate to address all of the individual entity's specific business activities; whether these controls are properly designed for the purposes of detecting, deterring and mitigating the particular fraud risks to which the entity is exposed; and whether these controls are being applied properly to sufficiently address the entity's unique business operations and fraud risks.

Deutsche Bahn AG is one example of a Transportation & Logistics company that has acknowledged the existence of fraud and taken active steps to combat it. Company executives have made compliance activities a matter for the highest management level, and the company's anti-corruption programme, launched in 2000, has a systematic structure and model character which have attracted national and international attention. Annual corruption reports are made available to the public and the company has set up ombudsmen and a compliance steering committee in order to facilitate reporting fraud and taking appropriate action when it is discovered.

Who watches the watchman?

Once fraud risk has been assessed and procedures put into place or refined to mitigate it, executives need to ensure that a comprehensive and functioning oversight system is in place.

The audit committee and the board, in performing their fiduciary duties, are responsible for considering their own knowledge of the company's underlying performance, the types of fraud prevalent in the sector and the risk of financial fraud by management, and ensuring that controls or mitigating actions have been taken to prevent and detect fraud. The audit committee and the board should consider management's risk assessment processes, specifically including consideration of the following:

- The process for identifying and documenting fraud risk
- The types of fraud considered by management (fraudulent financial reporting, misappropriation of assets, unauthorised or improper receipts and expenditures, and fraud by senior management)
- The level at which risk is considered (company-wide, business unit and significant account)
- The level of likelihood of fraud (probable, reasonably possible and remote)
- The level of significance of fraud (inconsequential, more than inconsequential or material)

An organisation should have a documented process that assesses, identifies and evaluates fraud risk. Audit committees should have an open and candid dialogue with the independent auditors regarding management's risk assessment process and the system of internal controls, specifically including a discussion of:

- The susceptibility of the entity to fraudulent financial reporting
- The exposure to misappropriation of assets or unauthorised receipts and expenditures
- The committee's views about the risks of fraud and the risk of override of controls by management
- Whether the committee has any knowledge of suspected or actual fraud

In addition to the high-level oversight of the audit committee, ongoing monitoring occurs in the course of operations and should be built into the normal, recurring operating activities of an enterprise. It includes regular management and supervisory activities and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of fraud risks and the effectiveness of ongoing monitoring procedures. Since separate evaluations occur after the fact, problems will be identified more

quickly by ongoing monitoring routines. Separate evaluations will ordinarily be conducted by the internal audit department or equivalent function. It is essential that the organisation's plan, approach and scope of monitoring activities be documented and reviewed from time to time.

We should note here that audit committee and supervisory board members who do not adequately address the possibility of fraud and ensure that their organisation is appropriately protected against the risk of fraud may be making themselves liable to civil or criminal prosecution.

Expertise and openness are key

Uncovering and dealing with fraud is not always straightforward. Companies should also ensure that specialists in the topic of fraud, be they internal or external, are an integral part of the organisation's team.

Perhaps the most effective weapon against fraud is open communication; executives need to ensure that they speak openly about fraud and don't attempt to hide instances when they occur. By demonstrating that the company takes fraud seriously, executives gain the trust of honest employees and deter potential fraudsters.

Overconfidence may pave the way for confidence men

Only a quarter of companies surveyed expect to suffer from economic crime – and 45% have experienced some type of fraud over the past two years. Add to this the fact that more than two-thirds of Transportation & Logistics respondents (69%) see the past two years as a particularly dynamic period of changes for their companies, and you have a potential recipe for trouble. Periods of intense change often create serious challenges for a company's internal control system. As an organisation grows more complicated, enters new markets or integrates new acquisitions, internal control systems may have trouble keeping up. And this in turn can lead to increased opportunity for fraudsters. Executives should acknowledge the risks posed by fraud and take action to minimise their companies' exposure.



Appendix – results of the Global Economic Crime Survey 2005

PricewaterhouseCoopers' Global Economic Crime Survey 2005 was based on interviews with executives responsible for detecting economic fraud in 3634 companies in 34 countries. This appendix is based upon interviews conducted with 119 Transportation & Logistics companies in 26 countries.

Economic crime is a significant issue

Nearly half (45%) of organisations in the Transportation & Logistics industry report have experienced economic crime over the past two years. Although the overall percentage of organisations reporting economic crime is in-line with the global average, Transportation & Logistics companies actually report a larger number of incidents of economic crime.

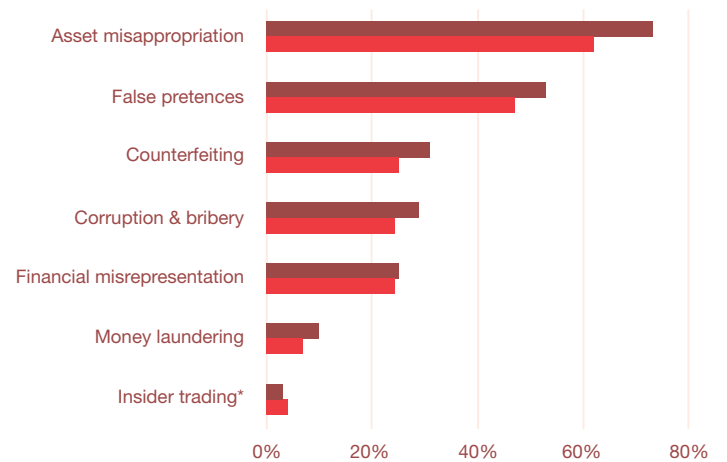
The nature of economic crime

The economic crime reported by far the most widely by those Transportation & Logistics respondents in our survey to have suffered a fraud in the last two years was asset misappropriation, named by nearly three-quarters of respondents (73%). Reports of this type of crime were somewhat less prevalent across our survey sample as a whole (62%). This high result may be due to the nature of the transport process, where goods are subject to multiple points of transfer which may provide opportunities for theft.

More than half of respondents experiencing fraud also reported instances of false pretences, and a significant percentage of companies have been affected by counterfeiting (31%), corruption and bribery (29%), and financial misrepresentation (25%) as well.⁵ In all cases, the percentage of Transportation & Logistics companies reporting having been subjected to this type of crime slightly exceeds that of our overall survey sample (see Figure 1).

The large number of companies reporting financial misrepresentation – one quarter of respondents overall – is particularly unsettling, given the seriousness of this type of offense.

Figure 1: Number of companies reporting different types of economic crime



Source: 2005 PwC Global Economic Crime Survey

* only listed companies were asked for insider trading

■ T&L Worldwide

■ Global (All Industries)

Costs of economic crime

Our survey results show that the average cost of tangible fraud (asset misappropriation, false pretences and counterfeiting) in the Transportation & Logistics industry is around US \$340,000. Incidents of asset misappropriation cost the Transportation & Logistics industry much less than other industries, perhaps due to the prevalence of cargo theft during the logistics processes. Cargo theft may more often involve relatively small sums, in contrast to more elaborate fraud schemes. The overall costs may still be higher than they first appear, however, given the fact that the number of incidents of crime for Transportation & Logistics is substantially higher than the overall average.

Specific incidents can have a major impact on Transportation & Logistics companies. When asked about the two most serious past incidents of crime in connection with their companies, 20% of Transportation & Logistics companies worldwide described the impact of the financial losses on their organisation as “very serious”, compared to only 9% of companies overall (see Figure 2).

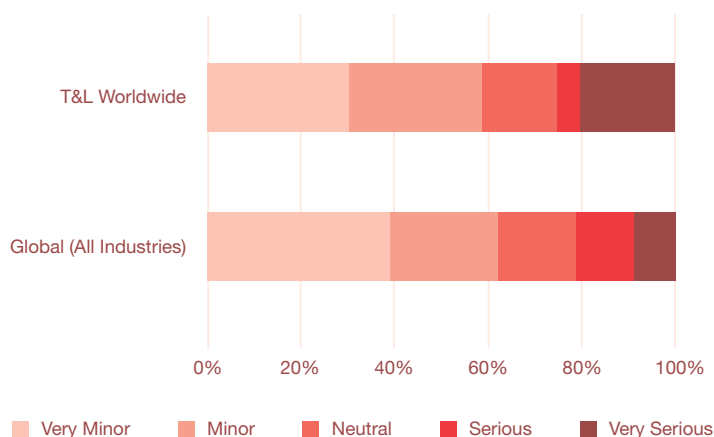
⁵ Relevant definitions of the types of crimes referred to in this supplement can be found in the Global Economic Crime Survey 2005, which is available for download at www.pwc.com/crimesurvey.

Intangible damages may also be a problem for companies experiencing economic crime – albeit one that often goes unacknowledged. Most Transportation & Logistics companies do not report significant amounts of intangible damage due to fraud – only 7% rated the amount of intangible damage as “high”, and 58% estimated that no intangible damages were incurred by the company.

Transportation & Logistics executives may well be underestimating the extent to which their companies are impacted by intangible factors. While most executives only think of the financial damage (when they think of fraud at all), in many cases the impact can be much more wide-reaching. If economic crime has an impact on relations with your staff (motivation), your clients (brand/reputation) and your suppliers (business relations), then you are affecting every working relationship that you have.

When asked if serious past incidents of crime had been made known to an external body, 41% of Transportation & Logistics respondents reported that customers or clients knew about the crime (compared to 29% of respondents overall). Furthermore, 73% of these incidents of crime were made known to law enforcement authorities, again exceeding the overall average of 64%. Around half of Transportation & Logistics respondents reported intangible damages resulting from serious incidents of economic crime, including loss of company reputation/brand (48%), decline in working morale (53%), and impairment of business relations (47%). Nonetheless, most Transportation & Logistics companies did not view the intangible damages the case had on their organisation as serious; a full 45% estimated the intangible damages as “very minor”.

Figure 2: Estimates of the impact of the financial losses of the most serious incidents of economic crime



Source: 2005 PwC Global Economic Crime Survey

Companies may be underestimating the extent to which morale, business relations and brand equity may be impacted by specific instances of fraud and by economic crime in general, particularly given the prevalence of serious types of crime such as financial misrepresentation, counterfeiting and money laundering.

Detection

Economic crime remains very difficult to detect. Despite most companies reporting a very high level of satisfaction with their various fraud detection measures, more than a quarter of frauds in the Transportation & Logistics industry are still detected by chance (e.g., through tip-offs or by accident). In fact, chance is the single most common means of detecting frauds in the sector. Internal audits also uncovered a number of frauds (25%).

Transportation & Logistics companies report a somewhat more successful corporate security function than our overall survey sample – more than three times as many frauds were detected by corporate security (14%), compared with an overall average of just 4%.

Fraud’s perpetrators

Although many companies may perceive economic crime as a third-party threat, more than half of the perpetrators of fraud (56%) were their own employees. This number is slightly higher than our global result and highlights the care companies need to take to understand more fully why their own employees may engage in economic fraud. While somewhat fewer perpetrators came from top and middle management in the Transportation & Logistics industry, two-fifths of perpetrators still fell into these categories. Fraud perpetrated by management tends to de-motivate staff. Senior management are also more likely to be dealing with significant figures in terms of financial damage, and more likely to undertake actions that seriously affect the brand and become public knowledge.

The 2005 survey also explored the motivations behind fraud for the first time. The four factors that respondents from the Transportation & Logistics industry identified as most important in motivating offenders included an expensive lifestyle, an easy to tempt perpetrator, lack of awareness of wrongdoing, and insufficient internal controls. (See Figure 3). When looking to the future, companies ranked these factors as somewhat less important. There may be a particularly important message here regarding internal

Figure 3: Top reasons for committing fraud



controls; only 31% of companies reporting a high willingness to increase fraud prevention through internal controls, perhaps due to a perceived lack of understanding of the extent to which insufficient internal controls provide opportunity to an enterprising fraudster.

Interestingly, when companies were asked to rate their willingness to increase crime prevention over the next two years through various measures, more than half (56%) expressed an interest in improving the internal audit function. Conversely, though only 31% were willing to focus on internal controls, despite the fact that internal audit can only perform optimally in an environment with sufficient controls in place.

Companies were also keen on increasing crime prevention through ethical guidelines/code of conduct – nearly half (47%) rated their willingness on this measure as high. At the same time, though, only 28% were looking to their compliance systems. While ethical guidelines and a code of conduct are a good starting point, these can only function effectively if all employees understand and are committed to them. Without effective compliance systems, these guidelines may all too often be disregarded by employees.

Reporting, investigations, recovery

Once fraud has been uncovered, companies need to decide how to deal with the perpetrator, and attempt to recover the lost assets.

Upon the discovery of fraud, and consistent with the global results, the most common response of Transportation & Logistics organisations was to inform their Boards of Directors (84%) and launch an internal investigation (84%). The majority of cases were also reported to law enforcement agencies (75%). Transportation & Logistics companies were somewhat more likely to call in external lawyers than their counterparts in other industries (45% compared to 36% globally), but were less likely to call in forensic accountants (18% compared to 22%) and other investigators (11% compared to 16%). While a willingness to deal with legal issues is laudable, Transportation & Logistics companies may do well to consider increasing the participation of other external experts as well.

In terms of measures taken against the perpetrator, Transportation & Logistics companies were somewhat more likely to dismiss, seek criminal charges, or take civil action against the perpetrator. Taking consistent sanctions against fraudsters is important in deterring future fraud, so this willingness to deal with the consequences of economic crime is a positive sign for the industry – particularly since only 3% of Transportation & Logistics companies chose to do nothing, compared to 13% of companies overall.

Transportation & Logistics companies made recoveries broadly in line with the global survey, with around half of companies (50%) recovering at least some of their losses. We should note here that cargo theft, probably the single most common type of economic crime in the industry, often remains undiscovered until the arrival (or non-arrival) at the destination. Offenders usually have time to dispose of goods before the loss is discovered, as most stolen goods are disposed of within 24 hours. These delays make recovery less likely.

Levels of insurance were slightly lower than the global average, and as noted previously Transportation & Logistics companies were somewhat less likely to call in forensic accountants than their counterparts in other industries, both measures which might help improve this picture with respect to some types of crime.

Management awareness

When asked to rate management’s knowledge of the causes of economic crime, only 16% of Transportation & Logistics organisations believed it was very good, and even fewer believed that their management had very good understanding of measures of crime prevention (7%). In addition, less than 30% of respondents rated management’s understanding of local corruption legislation as good or very good (29%), and over a quarter (26%) described knowledge of local corruption legislation as completely insufficient. If management are unaware of local corruption legislation, they may fail to notice or understand violations of such legislation within their own company. The level of good or very good knowledge of other economic crime legislation locally was slightly better (44%), however substantial room for improvement remains.

While it may not be relevant for all companies, we should note here the abysmal level of knowledge of the US Foreign Corrupt Practices Act (FCPA), which makes it unlawful to pay bribes to foreign officials and enhances accounting provisions and which is currently being strictly enforced by the US Department of Justice. Not one Transportation & Logistics respondent believed that company management had good or very good knowledge of the US FCPA and 25% of respondents reported that their management had completely insufficient knowledge of this law. Given that a significant number of Transportation & Logistics companies report having been subjected to corruption & bribery (29%), and many operate in the US, this response is worthy of note.

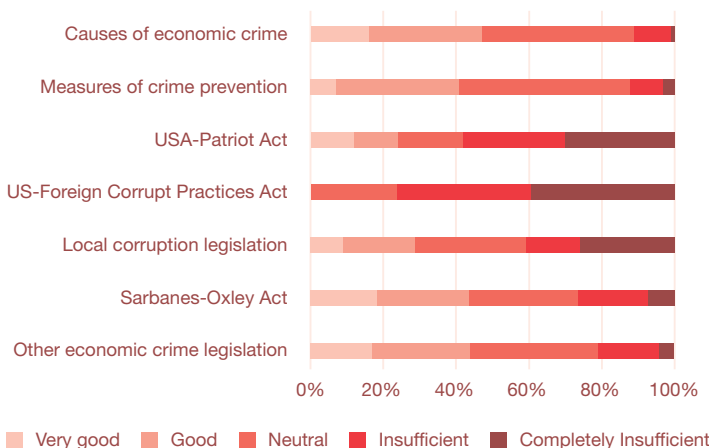
Senior managers need to do more to ensure that they have up to date knowledge in the area of economic crime, and in particular that they are knowledgeable about the strictures of local legislation and possible applications to their companies.

Notes

Full details about the methodology and demographics of the survey along with definitions of the terminology can be found in the [Global Economic Crime Survey 2005](#) report, which can be downloaded from the dedicated crime survey website at www.pwc.com/crimesurvey.

Transportation & Logistics companies participating in the survey were located in the following countries: Australia, Austria, Belgium, Bulgaria, Canada, Czech Republic, Germany, Hungary, Indonesia, Italy, Japan, Malaysia, Mexico, Netherlands, Norway, Poland, Romania, Russia, Singapore, South Africa, Spain, Sweden, Switzerland, Thailand, UK, USA.

Figure 4: Estimated level of knowledge amongst management of various issues



Source: 2005 PwC Global Economic Crime Survey

PricewaterhouseCoopers

global Transportation & Logistics

contacts

PricewaterhouseCoopers' Transportation & Logistics practice provides industry-focused assurance, tax and advisory services to public and private Transportation & Logistics companies throughout the world. For more information about this report, please contact the Transportation & Logistics leader in your country.

Australia

Don Munro
+61 2 8266 7328
don.munroe@au.pwc.com

Greece

Vassilios Goutis
+30 210 687 4620
vassilios.goutis@gr.pwc.com

South Africa

Akhter Moosa
+27 12 429 0546
akhter.moosa@za.pwc.com

Belgium

Peter van den Eynde
+32 3 259 33 32
peter.van.den.eynde@be.pwc.com

India

Amrit Pandurangi
+91 11 5135 0505
amrit.pandurangi@in.pwc.com

South America

Henrique Luz
+55 11 3674 3897
henrique.luz@br.pwc.com

Canada

Michael Whitworth
+1 514 205 5269
michael.whitworth@ca.pwc.com

Italy

Luciano Festa
+39 6 57025 2465
luciano.festa@it.pwc.com

Spain

Miguel Martin Rabadan
+34 91 568 4172
miguel.martin.rabadan@es.pwc.com

Central and Eastern Europe

Aleksander Domaradzki
+48 22 523 4160
aleksander.domaradzki@pl.pwc.com

Mexico

Martha Elena Gonzalez
+52 55 5263 58 34
martha.elena.gonzalez@mx.pwc.com

Sweden

Claes Thimfors
+46 31 7931131
claes.thimfors@se.pwc.com

China/Hong Kong

Alan Ng
+852 2289 2828
alan.ng@hk.pwc.com

Middle East

Nasir Hasan
+971 4 30 43 31 45
nasir.hasan@ae.pwc.com

Switzerland

Andreas Baur
+41 58 792 53 56
andreas.baur@ch.pwc.com

Denmark

Bo Schou-Jacobsen
+45 39 45 36 39
bo.schou-jacobsen@dk.pwc.com

Netherlands

Michel Adriaansens
+31 10 4075 271
michel.adriaansens@nl.pwc.com

United Kingdom

Clive Hinds
+44 1727 89 2379
clive.p.hinds@uk.pwc.com

France

Jean-François Châtel
+33 1 56 57 83 25
jean-francois.chatel@fr.pwc.com

New Zealand

Grant Burns
+64 9 355 8034
grant.burns@nz.pwc.com

United States

Kenneth H. Evans Jr.
+1 305 375 6307
kenneth.evans@us.pwc.com

Germany

Klaus-Dieter Ruske
+49 211 981 2877
klaus-dieter.ruske@de.pwc.com

Singapore

Subramaniam Iyer
+65 6236 3058
subramaniam.iyer@sg.pwc.com

We would like to thank the project team for their excellent and inspiring work: Herbert Nuszpl and Arno Hess for their valued contribution on forensic and fraud risk aspects, Steffen Salvenmoser for his assistance with analysing the results of the Global Economic Crime Survey, Peter Kauschke for project management and especially Elizabeth Montgomery, who did much more than just editorial work - without her, this report would not have been possible. Special thanks also to numerous members of the Transportation & Logistics industry network who provided feedback and input and supported this project with their knowledge and industry experience.

