Deloitte.

International Association of Airline Internal Auditors
IAAIA

Deloitte Airline Fraud Report 2010
Time to stop the losses

Contents

Foreword

Airlines exist in a volatile, dynamic market where competition is fierce and profit margins are tight. Anything that can damage a company's performance or reputation – including fraud – therefore demands attention.

The 2009 Deloitte Airline Fraud Survey took place at a time when airlines were operating at the bottom of the cycle, following the global economic recession, and we would therefore have expected them to be keeping a close eye on avoidable losses.

Our findings reveal that a third of airlines believe fraud to be a significant problem, and one that has increased in the past year. The results of the survey make intriguing reading for anyone working in the industry.

I would like to thank Deloitte for co-ordinating this project on behalf of the IAAIA and for providing this valuable report. I would also like to thank all those working in the industry who took the time to complete the survey.

Andrew Fisher
Chairman of the IAAIA

As in the 2006 survey, we wanted to engage with the global airline industry, and to find out whether people thought fraud had declined, increased, or remained the same – and to discover the biggest threats.

We were surprised in some cases to find that so many of our respondents still do not have a system in place to detect and track fraud and that only half of the airlines who responded give staff any training in this important area.

Our most recent findings were presented at the IAAIA annual conference in Abu Dhabi at the end of 2009 as part of a panel discussion. Responses from delegates have been incorporated into this report, adding more depth to our findings and highlight the most critical areas for concern.

We also used the conference to discuss ways of dealing with fraud, so that airlines could make their businesses more secure.

Deloitte would like to thank everyone who contributed to the survey and to the findings in this report.

Jean-Pierre Garitte
Partner, EMEA Enterprise Risk Services
EMEA Internal Audit Practice Leader

Executive summary

Top five fraud factors

1. Credit card transactions.
2. Economic pressure.
3. Organised crime.
4. Weak technology.
5. Lack of resources dedicated to fraud control.

Fraud hot spots

- 48% of those surveyed say that online fraud had increased in the past year.
- 35% are seeing more fraud through hand-held inventory and point of sale devices.
- 22% have seen an increase in the number of attempts to breach IT security and firewalls.

In the three years since our last survey, airlines around the world have been challenged by the worst economic crisis in a generation. The International Air Transport Association (IATA) suggests that two or three years of growth in international air travel were lost due to the recession, and the decline in passenger numbers coincided with an increase in fuel prices, plus growing pressure from the green lobby to minimise business travel.

There had already been a substantial amount of consolidation during 2009, with the industry braced to lose around US$5.6 billion in 2010. This was further exarcebated when the Icelandic volcano erupted in April, pumping ash into European airspace.

The ensuing chaos in the next six days was described by the International Civil Aviation Organisation (ICAO) as more disruptive to global air travel than the shutdown after 9/11, with airlines reportedly losing US$200 million a day.

At the peak of the crisis, it was reported that around a third of global flights were affected and estimated the total loss to the industry of around US$1.7 billion.

During the shutdown, shares in major airlines dipped, and there were reports that the loss of business was pushing some airlines towards bankruptcy.

Against this difficult backdrop, our global survey has revealed that each airline is still haemorrhaging an average of more than US$2.4 million a year on fraud.

More than half of the people we surveyed believe that fraud is a serious problem and is getting worse. The biggest threat comes from credit card crime, highlighted in our 2006 survey, which has been rising steadily along with the popularity of online bookings.

Airlines are now citing credit cards as the number one fraud risk factor, and almost half the airlines we surveyed said that fraud through electronic commerce and the Internet has increased within the past year.

Nobody can afford to ignore these losses, especially businesses that operate with such tight margins and in such a competitive industry.

Airlines are now citing credit cards as the number one fraud risk factor, and almost half the airlines we surveyed said that fraud through electronic commerce and the internet has increased within the past year.

Participants

Airlines from across the world agreed to take part in our survey, covering all sizes and business models. Personal invitations were sent out to heads of Internal Audit, or – for some of the smaller airlines – Directors of Finance.

Comments came back from all continents, and from network carriers, low cost carriers and charter companies.

The average number of aircraft owned by each operator was 156 and the average number of employees was 20,000. This compares to 127 aircraft and 13,700 employees in 2006.

The average turnover this time around was US$4.8 billion, compared to US$4.4 billion three years ago and US$1.9 billion in 2000, indicating the changed profile of participating airlines.

In 2006, the average loss due to fraud was estimated at US$3.3 million; whereas today it sits at around US$2.4 million. Of course, for some of the world's major airlines, the figures would be much higher, even though it would still be a relatively small figure at the bottom of a spreadsheet.

However, the real cost of the losses to fraud goes a lot further than the figure that appears on the books, as any concerns over an airline's security can have a highly negative impact on the image of the company. It can also damage relationships with suppliers and harm the workplace culture.

Across the board

While analysing responses to the survey, it became clear that the risks from fraud – and ways to manage them – could be divided into four distinct areas.

First: the Business Practice, or policies and procedures that determine the way an organisation operates.
For instance, the survey checked how many respondents have a clear fraud reduction plan or a code of ethics for staff to follow.

Second: Technology. Responses confirmed that airline information systems are highly vulnerable to fraud, and yet almost half of those we surveyed do not have a dedicated system to track or manage fraudulent attacks.

Third: Management Information. Business leaders have to understand and measure what's going on across their organisation, and without timely, accurate, centrally-managed information, airlines cannot develop robust prevention strategies.

Fourth: People and Training. Information gathered during the survey made it clear that staffing levels and employing people with the right skills are two important concerns.

Business practice

The 2006 survey revealed that around 65% of airlines had no policy for tackling fraud. Around the same percentage had no formal system to track abuse, nor did they carry out regular risk assessments.

In 2009, 35% still had no form of fraud policy at all, but 22% are in the process of creating one, and 43% of airlines say they have a fraud policy. However, when asked if they had a defined plan to reduce the amount of fraud, 70% said they hadn't.

An area that has significantly improved in the last three years, though, is the introduction of a whistle blowing mechanism to alert management to fraud. Back in 2006, 63% told us they had no such mechanism, whereas today, the same percentage of respondents say that they do and 8% were in the process of implementing one.

Just under a third – 29% – still have no whistle-blowing mechanism, but this shift in figures is encouraging.

A code of ethics is another useful tool in the fight against fraud, as it sets out what the company expects of its employees, and 75% of respondents have one. Although 8% of airlines don't have a code, 17% recognise its value and are in the process of developing one.

Clearly, having the right mechanisms and codes embedded within the company helps to create a culture of trust, which will have implications for employee morale as well as customer loyalty.

However, from the discussions we had at the IAAIA conference, it seems a code of ethics means different things to different people. Some airlines believe it constitutes a policy on fraud, while others see it as a way of setting the behaviour patterns of its employees. Meanwhile, others regard their fraud policy as synonymous with a code of ethics.

In reality, companies need both a fraud policy to tackle this particular threat, and a code of ethics to cover the way employees conduct themselves, and although the two are linked, they need individual attention to make sure they are clear and fit for purpose.

Keeping the lid on

More than a third of those we surveyed saw fraud as a serious and growing risk to the business. If airlines want to minimise these risks, it is imperative the business processes that govern the way things get done in an organisation are clear.

A fraud policy that covers the entire organisation should be agreed at the highest level, and then cascaded throughout the lines of business, giving business unit leaders the option of adding processes that are aligned with the overall group framework.

A Code of Ethics should also set the tone for standards of behaviour, so that employees know what is expected of them.

These two core elements, plus a whistle-blowing mechanism with clear instructions of how to report fraud – either from within the company or from suppliers or customers – should help to keep the lid on fraud.

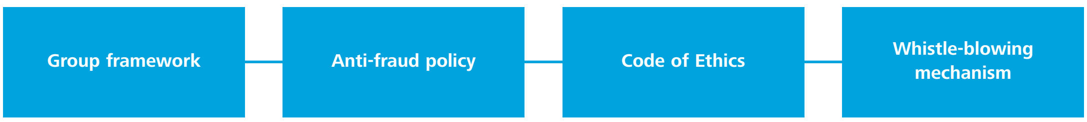
A fraud reduction plan, with clear objectives and goals, should be communicated across the organisation to encourage participation in the fight against fraud.

However, the factors that contribute to fraud are not static and airlines need to be aware of shifts in their business model and consumer buying preferences that could make them more vulnerable.

The steps to take

Developing a fraud detection plan:

- Understanding – a discovery phase will enable an organisation to identify where fraud is taking place and to priorities actions.
- Developing – having identified where the big risk areas are, airlines can develop a robust plan to remedy faults and put checks in place for ongoing monitoring.
- Make the change – this will focus on proven tactics and quick wins as well as longer-term strategies. Work should be ongoing, so benefits can be tracked as the solutions evolve and are implemented.



Technology

"There are massive commercial gains for airlines that allow customers to search for and buy their tickets online" says Jean-Pierre Garitte, "Self-service booking and barcode printing is much cheaper for the airline than booking via the phone or face-to-face.

"People today are prepared to shop around for schedules to suit them, and the advantages of 24-hour availability via the internet are obvious, however, customers demand high-speed service online and the application of the traditional credit card checks and anti-fraud controls can seem at odds with customers' expectations.

"It is therefore essential that the IT infrastructure that underpins an airline's commercial transaction is robust, and secure."

Losses through credit cards emerged during our 2000 survey, when they came third after tariff abuse and ticket theft. In 2006, credit card crime topped the table as the biggest risk area, followed by technology and web-based transactions.

In 2009, almost half of those we surveyed said that electronic commerce and internet fraud had increased in the past year and weak technology controls were still seen as a major threat.

35% of airlines said they had seen an increase of fraud attached to the use of point of sale or handheld devices and 22% said they had seen an increase in the number of attempts to breach IT security and internet firewalls.

The panel discussion at the IAAIA conference confirmed that fraudsters are becoming increasingly sophisticated in their ability to by-pass security systems, while the number of attacks was growing steadily.

Airlines told us that controls they had put in place to handle modern payments systems were not foolproof, and the speed of online transactions meant that some types of fraud could occur before internal checks had been applied.

Worryingly, 52% of those surveyed have no system to formally detect and track fraudulent attempts to obtain tickets, and only half of respondents had a formal system to pick up unusual transactions or suspicious activities.

More than 20% of airlines said they were not aware of the Payment Card Industry (PCI) standards to protect consumers from credit card abuse; and almost a third told us there was no system to check whether staff were going back into the system to retrieve a customer's credit card details.

Several respondents had no process for checking that names on tickets matched those on credit cards, or that a single card was being used for multiple purchases.

As airlines seek to use the expanding number of digital channels to interact with customers and business partners, they need to do more to safeguard their systems, and their customers' credit cards, from fraud.

A question of control

Enabling more people to connect into an airline's core IT system is a calculated risk, and this needs to be balanced with the commercial and competitive benefits of harnessing the latest technologies.

There are plenty of technology solutions that would enable airlines to make their systems more resilient to attack – from both inside and outside of the company – as well as applications that would monitor and report on fraudulent activities.

Many suppliers of counter-fraud technologies will evaluate the risks and provide free proof of concept applications, so airlines can see the business benefits before deciding whether to invest. A range of methodologies and techniques may need to be implemented to ensure the entire organisation is covered, but the right technology is an important weapon against fraud.

Currently, around 65% of surveyed airlines outsource their fraud management to third parties, and while outsourcing can be a more cost-effective option, it does mean relinquishing control over a critically-important aspect of the business.

At the least, any third party contract should include robust operating principles and service level agreements, ensuring that the legal requirements of the airline are covered as well as the integrity of its brand.

Providers should also provide regular and detailed reports that monitor and manage performance and effectiveness for business sponsors.

The steps to take

Only 50% of respondents have a system in place to identify, track and manage cases of fraud, but the dynamic pace of electronic commerce and interconnectivity makes such a system essential.

- Understand the organisation's needs – check the business requirements and align these with the risks.
- Develop the business case – a cost/benefit analysis will balance the investment needed to prevent a US$1 million loss through fraud.
- Implementation and smart working – fully embed new processes, controls and performance metrics.

Management information

The steps to take

Airlines can turn their data into valuable information by:

- Managing the massive amounts of data that come into the organisation, and use business intelligence to monitor and track fraud.
- A risk-based approach will enable companies to prioritise actions and become more cost-effective.
- Management reporting should cover the business from end to end, enabling business leaders to get accurate, timely information on what's happening and to make the right decisions.

The world is now more interconnected than ever, and businesses can now interact with customers, suppliers and business partners through numerous channels. As a result, large companies – including airlines – are often struggling to cope with the massive amounts of data they hold.

While most business leaders agree that all this data gives them a much better insight into their customer's buying habits and preferences, they would also agree that it's what they do with all this data – rather than the data itself – that makes it a real asset.

Companies today have often been described as having too much data – but not enough really useful information – because they often can't link up their IT infrastructure with the physical components of the business.

And although we talk about global strengths, quite often information is gathered and stored at country or functional level, so that the company is prevented from seeing a complete picture.

Our survey therefore investigated how airlines accessed their data, and questioned the effectiveness of their methodologies.

During the panel discussion at the IAAIA conference, delegates told us how they are developing fraud-reporting dashboards to integrate the entire risk hierarchy, from the Chief Risk Office (CRO) right down to the fraud investigators. Reporting benchmarks are set according to the objectives and focus of each department.

This, however, appears to be best practice for the industry, as only 50% of our survey respondents told us they had a dedicated management information (MI) programme which collated and reported incidents of fraud. We also found that only 54% of respondents accessed and reported MI regularly, usually on a monthly basis.

Ideally, MI should be transparent and timely, with consistency of all data and terms across the airline at a country, regional and global level. A direct line from source to use should be visible, to enable checks on the quality and integrity of that data to be performed.

Centrally managed data would maintain the consistency of reporting between regions, and regular reconciliations should be undertaken to ensure measurement baselines have not drifted.

This will ensure management are making fully-informed decisions, and any benefits are real and not imagined.

At the IAAIA conference, several airlines told us they had introduced tactics to spot suspicious activities, and had blacklisted certain individuals from buying tickets, redeeming frequent flyer points or from making bookings for third parties.

This might seem a good idea, but there is a risk of mistaken identity that could lead to negative repercussions on business and reputation. One way of mitigating the risk would be to ensure any blacklisting was refreshed frequently.

There is a case for the airline industry to adopt what has become common practice across the financial services sector – particularly insurers – with sharing data on known fraudsters, crime trends and suspicious activities.

We know that current airline systems deploy fraud indicators, and that major players also use external data sources, such as credit reference information and machine fingerprint identification, and the more an airline can discover about its customer's previous transactions, purchase types and buying history, the better.

With the global nature of business today, underpinned by the Internet, it's important that data sharing agreements should meet local data protection and compliance as well as global standards.

Our survey, for instance, found that fraudulent transactions were highest in the Far East, but making sure security checks meet regulations in the local country as well as the airline's head office can be complex.

Data protection experts would want to be assured that data was being used to fight against fraud rather than for future marketing and sales objectives.

Airlines need to manage their data in the most effective way, so they can see where the major risks are and take action accordingly.

Making people count

Back in 2006, we found that 60% of airlines were relying on Internal Audit to prevent, detect and investigate fraud, and yet the size of Internal Audit departments were among the smallest when compared to other industries.

64% of airlines were making do with an Internal Audit department of between one and ten people, compared with 20% of companies across the transport industry as a whole.

Fast forward to 2009, and 65% of respondents still believe staffing levels are too low, and there are not enough specialists investigating and handling fraud.

Delegates to the IAAIA conference said that recent reductions in headcount were generally due to the weak economy, however, the cost of employing staff needs to be balanced against the much larger costs – to profit and reputation – of fraud.

Half of the respondents to our most recent survey said their airline lacked the correct skills to fight fraud, and only 50% of airlines offered regular training to staff on how to identify and escalate suspicious activity.

This is a particular concern given the increasing sophistication of today's attackers, and that regular training would enable staff to keep up to date with emerging trends and shifts in customers' habits.

In our survey, we also wanted to find out how employees' management of fraud was linked to reward, and discovered that in 70% of cases a commitment to identifying and managing fraud is not part of an individual's appraisal. Contributors to our panel discussion suggested this was not an important topic during the annual performance reviews, although this could change.

This seems like an opportunity missed, as linking fraud management with the company reward scheme can motivate staff to take on challenging cases. Without this incentive, employees may ignore suspicious activities, particularly if getting involved means taking on a lot of extra work.

However, with the right structure in place, staff can be encouraged to own the issue of fraud and deliver against set targets. Implementing the necessary training and rewards structure can take a considerable amount of management time, but the results should be worth the investment.

Dedicated teams should be set up to focus on fraud, while every employee should have at least some basic knowledge of how to identify fraudulent activities. Fraud can occur across a number of areas, so it will pay to give employees a basic understand, perhaps during the induction process.

The steps to take

Empowering and training staff to deal with fraud will need:

- The right structure – analytical and operational staff should be encouraged to work together to manage existing threats and identify new ones.
- Continual training – All employees should have a basic level of understanding of the issues and how to deal with fraud. More in-depth training will be delivered to those working on the fraud frontline, and this should be continual, so that specialist knowledge keeps up with emerging threats.
- Recognition and reward – employees will respond if they are given ownership of fraud prevention, and if their detective work is rewarded.

Conclusion

The 2009 Deloitte Airline Fraud Survey built on the questions we put to airlines at the start of the decade and again in 2006 and presents us with a snapshot of fraud across the industry.

This year's results highlight four key areas of concern, which were further developed during the IAAIA annual conference, and which we have looked at in this report.

One of the most alarming facts to emerge is that, although fraud is regarded as a serious risk by many airlines, only half of those we surveyed have any formal system in place to track it. And while 48% feel that fraud through the internet or e-commerce has increased during the past year, weak technology controls are still blamed as a contributing factor.

Some of the world's major players may not lose any sleep over the US$2.4 million they say they are losing a year to fraud, and may see it as a consequence of the far more inter-connected and open business model they deploy in the digital world.

However, if the gaps are not plugged fairly swiftly and a lot of the steps we have outlined in this report don't happen, losses could rise as fraudsters find new ways to by-pass security and firewalls and un-trained, un-motivated employees turn a blind eye.

Of course, there are some airlines that are doing everything they can to prevent losses, but there are others who are not even aware of the Payment Card Industry standards, introduced in 2006 to protect consumers from credit card abuse.

Most businesses would agree that not taking full responsibility for the security of online transactions, and not having a robust anti-fraud programme in place raises questions about corporate governance.

A governance framework assures customers, suppliers and business partners of the quality of management within a company and – putting aside the financial costs of fraud – a tightly-controlled organisation will perform better.

Deloitte and the IAAIA would like to thank all of those who participated in our survey and who contributed to the debate at the conference in Abu Dhabi.

The information you gave us has enabled us to create a benchmark report that – we hope – will be of interest to all those working in the airline industry today.

Appendix

Methodology
Confidential invitations were sent out to the heads of Internal Audit for all the major airlines. For smaller companies, invitations were sent to Directors of Finance.

Around 50% of the IAAIA's member airlines participated.

Responses were summarised on an aggregate, collective, non-name basis.

Confidentiality has been maintained at all times.

Acknowledgements
We would like to thank the following people who provided us with their comments and insights:

Andrew Fisher	Etihad Airlines and Chairman of the IAAIA
Maurice Sammut	British Airways
Neil Berry	Deloitte
Jean-Pierre Garitte	Deloitte
Jacque Hawk	Deloitte
Mike Maddison	Deloitte
Andrew Morris	Deloitte
Neil Morris	Deloitte
Graham Pickett	Deloitte
Lisa Su	Deloitte
Amanda Toop	Deloitte
Kent MacKenzie	former Deloitte

We would also like to thank all those airlines who contributed to this survey. They will not be named to ensure confidentiality.

Contacts

Jean-Pierre Garitte
Partner, Enterprise Risk Services
EMEA Internal Audit Practice Leader
Mob: +32 475 947 256
Email: jpgaritte@deloitte.com

Graham Pickett
Partner, Audit
UK Aviation Leader
Tel: +44 1293 761232
Email: gcpickett@deloitte.co.uk

About Deloitte
Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 140 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's approximately 169,000 professionals are committed to becoming the standard of excellence.

About the IAAIA
The International Association of Airline Internal Auditors (IAAIA) began in 1991 with several airlines gathering in London to exchange information on challenges and best practices experienced within their Internal Audit departments. As of 2003, the organization has grown to over 70 member airlines and continues to meet annually all across the world to network, exchange ideas and solutions.

Notes

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom. Tel: +44 (0) 20 7936 3000 Fax: +44 (0) 20 7583 1198.

Designed and produced by The Creative Studio at Deloitte, London. 4739A

Member of Deloitte Touche Tohmatsu