

ascend

Taking your airline to new heights

THE POWER OF PARTNERING

A Conversation with
Abdul Wahab Teffaha,
Secretary General
Arab Air Carriers
Organization.



Special Section

Airline Mergers and Consolidation



INSIDE

21

Carriers can quickly recover from irregular operations

46

Singapore Airlines makes aviation history

74

High-speed trains impact Europe's airlines



An increase in fraud, especially through credit card use, is costing airlines millions of dollars each year, but the right technology can help control fraudulent activity.

■ By Tim Maher | *Ascend* Contributor

Advanced technology has played a significant role in helping airlines throughout the world reduce operating costs. Self-service check-in kiosks, Internet booking tools, and interactive voice response solutions not only assist carriers in their pursuit to achieve greater cost efficiencies, but also improve customer service and market differentiation. While most everyone will agree that technology has overall benefited the airline industry, there are some areas of concern — one in particular

being how it has increased the amount of fraud carriers incur.

According to the March 2007 issue of the Nilson Report, a leading payment systems publication, fraud losses in the United States last year incurred by issuers of American Express, Discover, MasterCard and Visa increased to US\$6.69 cents per US\$100 in purchase volume. When extrapolating this figure to the US\$325 billion in global passenger airline revenue in 2005, as noted in the July 2006

World Airline Report published by *Air Transport World*, the total amount of fraud incurred by the airline industry would exceed US\$217 million. That's certainly a figure that should garner a significant amount of attention within the executive offices of each airline, but according to a 2006 study by Deloitte and the International Association of Airline Internal Auditors, that's not necessarily the case.

The Deloitte study reported that fraud losses for carriers has increased fivefold over the previous



five-year period and that while fraud comes from two sources — internal and external — it is the external fraud, particularly credit card, that is more problematic and growing more rapidly, and accounted for 60 percent of all external fraud-related losses. The biggest culprit related to the growth of credit card fraud comes from Web-based transactions. While virtually every carrier is using the Internet as an efficient and effective way to market and sell their services directly to customers across the globe, it is also exposing them to greater amounts of fraud. According to the study, airlines suffer an average loss of greater than US\$1 million annually; however, the alarming part shows that 65 percent of carriers that participated in the study have no fraud program in place to detect or report fraudulent transaction activity.

Given that Web-based transactions are expected to grow, one can assume the level of fraud will also escalate. So what measures can airlines take to better manage fraud, particularly as it relates to their Web site? If an airline has not implemented a fraud solution, there are three steps that are a good place to start:

1. Understand how much fraud is costing. An airline should engage constituents throughout its organization (information technology, security, finance, internal audits, sales/marketing, etc.) and determine where the fraud exists, and more specifically, what it is costing. For example, how does fraud breakdown per credit card type? What are the characteristics of the itinerary? Several items should be reviewed, including:
 - a. What are the origins and destinations?
 - b. What are the classes of service?
 - c. What is the time between booking and the first leg of the itinerary?
 - d. What are the credit card numbers?
 - e. What e-mail addresses are used?

Ancillary costs such as personnel, bank fees and other expenses that may not be directly associated with the fraudulent transaction activity should also be considered. These costs should be analyzed regularly, just as all other expenses are monitored. By understanding the total cost of fraud, an airline can proceed to the second step, which is to develop a specific plan of action.
2. Develop a fraud plan. Formulating a plan of action is the most difficult part of implementing a fraud program. Airlines should consider engaging a fraud management consultant to assist with developing the plan. Regardless of whether or not a consultant is involved, several items should be considered as part of the plan:
 - a. Identify fraud tools that are easily accessible:
 - i. Address verification service is a tool provided by credit card associations that enables merchants to validate that the address provided by the

customer matches the address on file with the card issuer. This functionality was originally implemented in the era of mail order/telephone order sales and has been available in North America for many years, but is not necessarily a reliable or effective tool in today's virtual world.

- ii. Card security code is another tool provided by credit card associations that enables merchants to verify that the cardholder is in possession of a card by validating with the card issuer the three- or four-digit numbers that are separate from the card number. This functionality was implemented in the late '90s as e-commerce was becoming more mainstream. CSC has proven to be much more effective in identifying potentially fraudulent sales than AVS.
- iii. 3D-Secure is the latest tool provided by certain credit card associations as a way to provide greater security for online shopping. While the programs are commercially known as "Verified by Visa" and "MasterCard Secure Code," they work essentially the same way. When a consumer pays with a Visa or MasterCard at a 3D-Secure-enabled merchant, the consumer goes through a process known as a "trust chain" throughout the transaction, whereby the identity of the consumer is authenticated via a passcode that is known only to the consumer that is on file with the issuer. One of the most significant benefits associated with 3D-Secure is that the liability for fraud is shifted from the merchant to the issuer (under a range of conditions). Earlier this year, *Sabre Holdings*[®] partnered with Eurocommerce, a Dublin, Ireland-based payment services provider, to jointly offer the optional functionality of 3D-Secure to *Sabre Airline Solutions*[®] customers. India's Kingfisher Airlines recently implemented 3D-Secure within *SabreSonic*[®] Web as a way to reduce its exposure to fraud while extending its sales reach into new markets throughout the world.
- b. Investigate the use of a third-party fraud management solution to screen all Internet sales. CyberSource, eFunds, Fair Isaac, Retail Decisions and VeriSign are just a few examples of companies that offer such a solution, which scores a transaction for fraud potential based on dozens of different variables associated with the sale. Transactions that score above a certain level are escalated for alternative processing before the

sale is completed. Merchants have the capability to adjust the scoring thresholds based on the unique characteristics of their business model. While there is a cost associated with these services, they have touted their ability to reduce fraud to less than 0.5 percent, which for some airlines could mean hundreds of thousands or even millions of dollars in annual cost savings. *Sabre Airline Solutions* is analyzing the value its customers would receive if it partnered with a third-party fraud management company.

- c. Just as an airline engaged the appropriate constituents across its organization to understand its cost of fraud, it should also engage them in development of the plan. IT security will identify the technical aspects; internal audits will assist with controls and measures; and finance will develop the cost/benefit analysis. Ensuring that effective project management processes and personnel are in place is also a critical aspect of the plan. The plan should clearly depict the goals and objectives of the project.
3. Monitor progress. One of the biggest faux pas organizations make regarding a fraud management plan is that after implementation, they do not effectively monitor the progress to understand whether they are achieving effective results. All entities that were part of the planning process should also be involved in monitoring the progress. IT security should keep up with new technologies and their implications for fraud, internal audits should review the internal controls, finance should analyze the costs and financial benefits, and sales and marketing should assess the impact to sales and usability. A periodic review by all parties must result in the team adjusting strategies and/or processes to increase effectiveness, which will ultimately result in reducing the volume of fraud across a greater volume of sales.

While an in-depth action plan will certainly assist any business, not just airlines, in developing a strategy to combat fraud, it is important to recognize that there is no panacea for eliminating it. Fraudsters progressively get more and more sophisticated in their approach and use technology to increase their effectiveness. However, by taking action, airlines can effectively manage fraud while simultaneously increasing sales. **F**

Tim Maher is an account director for the Sabre Airline Solutions sales and account management team. He can be contacted at tim.maher@sabre.com.