CyberSource®
the power of payment

In association with AirlineInformation

2011 EDITION

Airline Online

FRAUD
REPORT

Online Payment Fraud Practices & Benchmarks
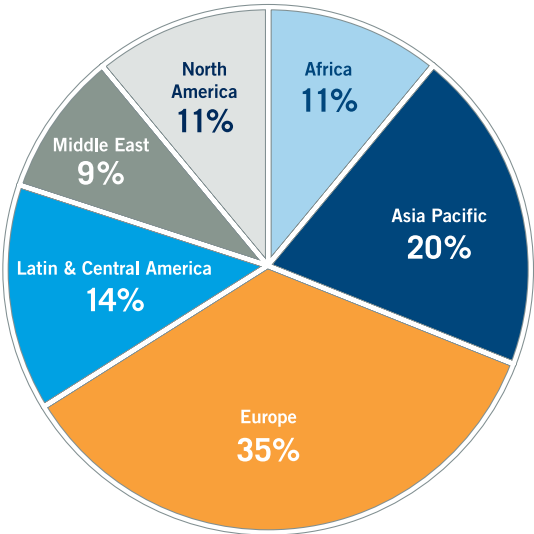
Report & Survey Methodology

The CyberSource Airline Online Fraud Report, developed in association with Airline Information, is based on a survey of airlines from across of the globe, representing an estimated 40% of total worldwide online sales. Decision makers who participated in this survey were either ultimately responsible for, or had significant influence on, fraud management policies and decisions for their carrier.

Online sales experience levels range from airlines with less than three years to over ten years experience selling via the web (see Chart #1). The airlines participating in the survey ranged in size from less than $500 million1 in total annual sales to over $10 billion. Online sales from airlines participating in the survey totaled $62 billion in 2010.

The survey was conducted via online questionnaire by handl Research and completed by 142 participants between November 17, 2010 and January 31, 2011.
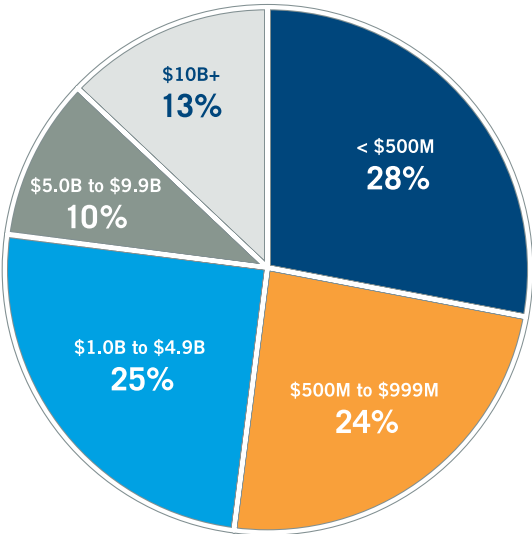
1. All $ amounts quoted are in USD

Summary of Participants' Profiles

1

Airline HQ Location

- North America **11%**
- Africa **11%**
- Asia Pacific **20%**
- Europe **35%**
- Latin & Central America **14%**
- Middle East **9%**

n=142

Annual Worldwide Revenue (USD Millions)

- $10B+ **13%**
- < $500M **28%**
- $5.0B to $9.9B **10%**
- $1.0B to $4.9B **25%**
- $500M to $999M **24%**

n=75

Risk Management Responsibility

- Ultimately Responsible **41%**
- Influence Decisions **59%**
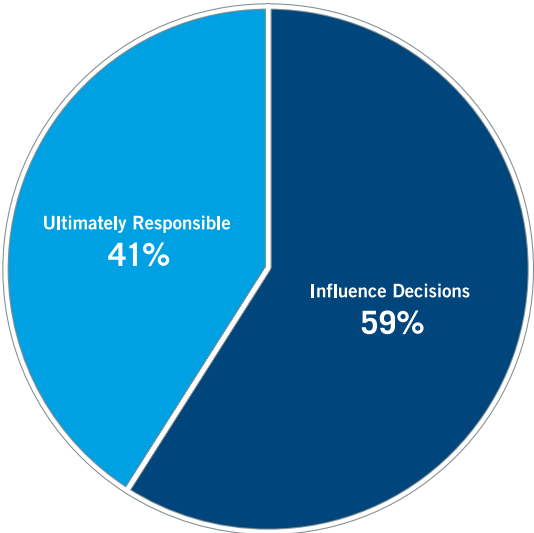
n=142

Duration of Online Selling

- 10+ Years **27%**
- < 3 Years **13%**
- 3–4 Years **10%**
- 5–6 Years **23%**
- 7–9 Years **27%**
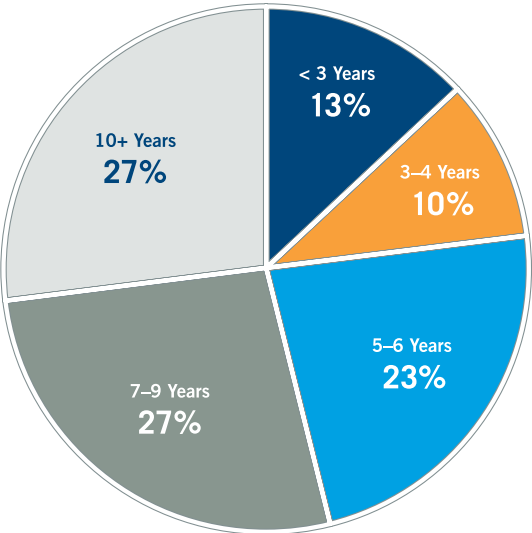
n=142

Table of Contents

Executive Summary

Airlines face distinct business challenges compared to other online merchants. To help airlines better understand payment fraud in their unique industry, CyberSource commissioned this survey to address the detection, prevention and management of online payment fraud. This report summarizes those findings and provides direction on fraud management practices.

Overview

For most of the world, 2009 and 2010 have been marked by a period of recession and subsequent slow economic recovery. Many companies, including airlines, focused their attention on cost-cutting measures during this period. Although airline ticket sales rebounded in 2010, loss due to online payment fraud is down since the last survey, in both percentage of overall online revenue and bookings.

In 2010, airlines worldwide lost an estimated $1.4 billion dollars in revenue due to online fraud perpetrated on their websites, which represented 0.9% of total worldwide online airline ticket sales. In comparison, airlines reported losing $1.7 billion in the previous survey2, representing 1.3% of total online airline ticket sales worldwide. This represents a 31% reduction in fraud loss rate from what was reported in the previous survey. However, over a quarter of airlines surveyed expected their fraud loss rate to be greater than 1% of their online revenue in 2010, suggesting there are still some airlines that could improve their online fraud management processes.

Based on how revenue loss was addressed in the survey, the fraud losses reported include losses for all payment methods together with fraud chargebacks from credit and debit cards.

The fraud loss rate is based on revenue derived from an airline's website only, and does not include card-present or telephone transactions, which are often included in the fraud loss metrics provided by card associations.

Finally, the loss rates reported in the survey include any losses due to the issuance of credits or refunds to customers to avoid chargeback disputes or to maintain goodwill— a common practice among non-travel online merchants. Credits may also be issued by a different airline department, which may not be responsible for chargebacks or merchant account management.

Fraud loss rates vary by online sales experience and type of airline. Airlines with less than three years of online sales experience have a fraud loss rate which is three times higher than airlines with more than ten years. This can be expected, given that airlines with more experience have been on the front lines longer, and are more likely to have better fraud tools and processes in place.

Looking at fraud loss by airline type, low cost carriers have one-third the fraud loss rate of full fare carriers (see Chart #2). Low cost carriers tend to have slimmer margins than full fare carriers, which may compel them to focus more strongly on deterring fraud. Fraud screening may also be less complex, as low cost carriers typically sell point-to-point fares (versus multi-leg trips) and may not have frequent flyer programs or multiple cabin classes to consider.

% of Website Revenue Lost to Online Fraud

2. 2008 figures have been adjusted to reflect revised analyst updates in overall revenue estimates.

Key Fraud Metrics

Beyond fraud loss rates, there are a number of other metrics to consider, such as online booking reject rate, manual review rate, and fraudulent booking rate. In the survey, online booking reject rate is the number of online bookings automatically or manually rejected for processing or cancelled prior to a flight departure, due to suspicion of payment fraud. Manual review percentage refers to the percentage of the bookings made on the airline's own website that require manual review to screen for online payment fraud. Fraudulent booking rate looks at the share of bookings that were accepted, but were later found to be fraudulent.

In 2010, airlines reported that on average, for every fraudulent website booking, they rejected an additional 5.1 bookings due to suspicion of fraud. Furthermore, the average online booking reject rate was 3.3%, in comparison to 2.8% in the previous survey. Over a quarter of airlines reported their online booking reject rates to be more than 5%.

The fraudulent booking rate averaged 0.65%, but varied widely by region and years of experience. Airlines in Latin and Central America had more than twice the fraudulent booking rate (1.4%), while airlines with less than three years of experience reported 1.6%.

Survey data also revealed that 26% of online bookings require additional manual review. Yet there is still a large percentage of airlines—20%—that do not conduct manual review at all.

22% of Fraud Losses are Recoverable

Airlines report that they win almost a third of the fraud chargebacks they re-present, resulting in an average net recovery of 22% of initial fraud chargeback claims. However, over a quarter of airlines surveyed report that they challenge fewer than 10% of initial fraud claims, while 42% challenge 70% or more of their initial fraud claims. Airlines that do not have an efficient process for fighting fraud claims are incurring additional unnecessary fraud losses.
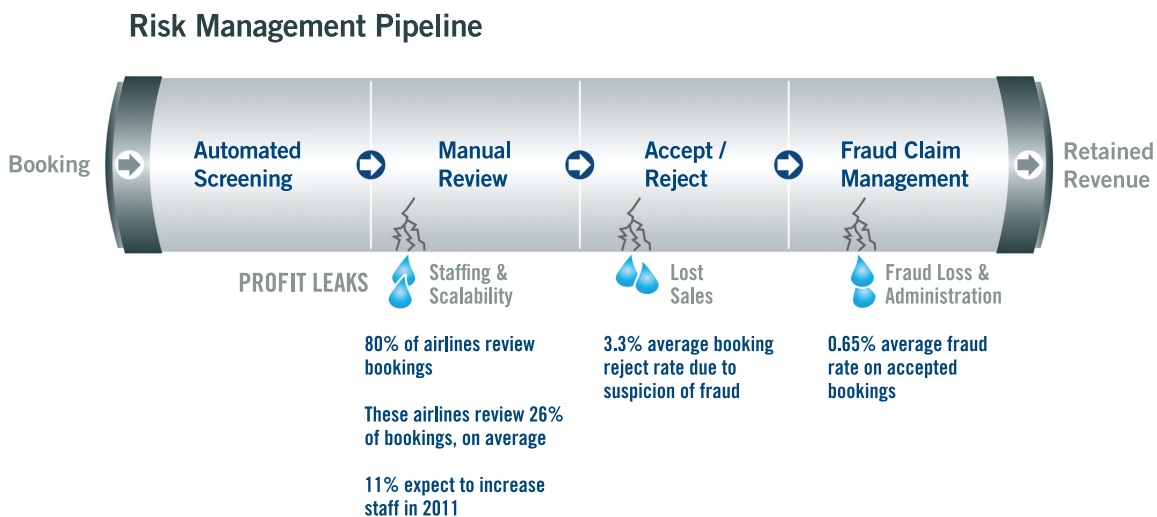
Efficiency Gains Required

As online sales continue to grow while budgets and resources remain relatively fixed, airlines face the challenge of screening more online bookings while keeping booking rejection and fraud rates as low as possible, to maximize sales and profits.

Total Pipeline View

Online payment fraud continues to impact revenue from online sales. However, other than direct revenue loss due to fraud, there are additional costs such as the rejection of valid bookings, the staffing of manual review teams, the administration of fraud claims and the challenges associated with business scalability. Inefficiencies and further profit loss can occur if the airline's payment fraud processes and the above costs are not carefully managed.

Airlines can gain efficiency by taking a total pipeline view of operations and costs. While the fraud rate is one metric to monitor (and contain within industry and card brand limits), an end-to-end view is required to arrive at the best possible financial outcome.

In 2010, "profit leaks" in the Risk Management Pipeline™ impacted as much as one quarter of online bookings—restricting profits, operating efficiency and scalability. This report details key metrics and practices at each point in the pipeline to provide benchmarks.

Risk Management Pipeline

Booking → Automated Screening → Manual Review → Accept / Reject → Fraud Claim Management → Retained Revenue

PROFIT LEAKS

Staffing & Scalability
Lost Sales
Fraud Loss & Administration

80% of airlines review bookings

These airlines review 26% of bookings, on average

11% expect to increase staff in 2011

3.3% average booking reject rate due to suspicion of fraud

0.65% average fraud rate on accepted bookings

Stage 1: Automated Screening

Fraud Detection Tools

Fraud detection tools are defined as those used to validate purchaser identity or identify the risk associated with an online transaction. Today, a wide variety of tools are often used in combination to help airlines evaluate incoming online bookings for potential fraud. These tools can be grouped into four main categories: global validation services, single airline purchase history, purchase device tracing and multi-airline purchase history. Information from these tools is evaluated either by a fraud review staff or an automated rules engine, to determine whether a transaction should be accepted, reviewed or rejected.


To better understand when fraud screening generally takes place, airlines were asked to indicate the order of five key steps in the booking process: booking generated, payment authorization, booking screened for fraud, ticket issuance, and payment settlement. As Chart #3 demonstrates, airlines in this survey vary greatly in terms of when they screen for fraud.

On average, airlines reported using 7.3 fraud tools (see Chart #4). As expected, carriers with ten or more years of online sales experience reported a higher than average number of fraud tools used and saw lower fraud loss rates than carriers with less experience.

The tools with the highest adoption include Card Verification Number (CVN), negative lists, IP geolocation information, and Verified by Visa/MasterCard SecureCode (see Chart #5). Shared negative lists/hotlists are also popular, and reflect recent trends seen in terms of airlines wanting to share and leverage collective knowledge across the industry.

Validation through social networking sites, a relatively new tool for fraud detection, is in use by only 8% of airlines. However, adoption may increase as social networking continues to grow in popularity.

Yet there is a difference between fraud tool adoption and perceived effectiveness. To eliminate bias toward the more commonly used tools, the data was normalized by evaluating the top tool choice against those airlines using that tool. Out of the five fraud tools with the highest adoption, only two were identified in the top five for perceived fraud tool effectiveness — shared negative lists/hotlists and Verified by Visa/MasterCard SecureCode. For the latter, adoption is most likely due to more favorable interchange, whereas effectiveness is likely due to liability shift.
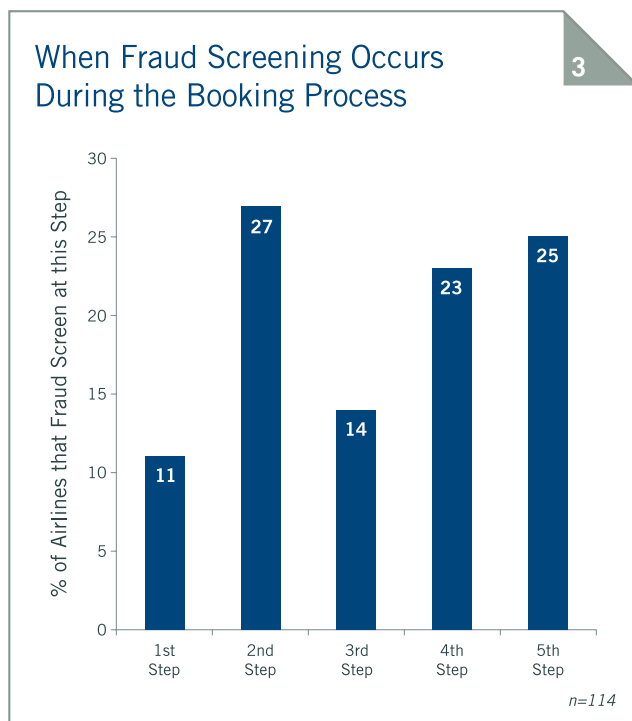
Airlines with large online booking volumes typically evaluate incoming bookings automatically to determine the fraud risk. Based on the results of this initial risk screening, bookings are then assigned one of three states: accept, decline or suspend for further review.

Average Number of Detection Tools Used

4

Category	Value
Total	7.3
< 3 Years	6.4
3–4 Years	6.8
5–6 Years	7.0
7–9 Years	7.7
10+ Years	7.8
Full Fare	7.3
Low Cost	7.2

Years Selling Online   Airline Type

n=120

Fraud Detection Tools – Current Usage

5

Validation Services
Tool	%
Card Verification Number (CVN)	79
Verified by Visa/MasterCard SecureCode	60
Address Verification Service (AVS)	36
Telephone number verification/reverse lookup	27
Postal address validation services	18
Credit history check	16
Validation using social networking sites	8
Paid for public records services	3
Out-of-wallet or in-wallet challenge/response	3

Single Airline Purchase History
Tool	%
Negative lists (in-house lists)	76
Order velocity monitoring	47
Positive lists	45
Customer order/Frequent flyer history	40
Fraud scoring model – company specific	36

Purchase Device Tracing
Tool	%
IP geolocation information	63
Device "fingerprinting"	13

Multi-Airline Purchase History
Tool	%
Shared negative lists/hotlists	48
Fraud scoring model – third party	44
Other	8

% of Airlines   0 10 20 30 40 50 60 70 80 90

n=120

4

Although CVN has the highest adoption, only 24% of airlines in the survey considered it one of their top three most effective tools (see Chart #6). In this instance, adoption may be due to CVN being an integral part of conducting eCommerce, along with interchange benefits.

Neither out-of-wallet/in-wallet challenge response nor validation using social networking sites was considered by the airlines to be among their top three tools. The challenge response system can be costly and difficult to implement on a global basis, particularly with respect to localization, quality, and depth of information available internationally.

Most Effective Fraud Detection Tools as Perceived by Airlines   6

Validation Services

Tool	%
Verified by Visa	60
Paid for public records services	50
MasterCard SecureCode	46
Card Verification Number (CVN)	24
Credit history check	16
Telephone number verification/reverse lookup	16
Address Verification Service (AVS)	12
Postal address validation services	5
Validation using social networking sites	0
Out-of-wallet or in-wallet challenge/response systems	0

Single Airline Purchase History

Tool	%
Negative lists (in-house lists)	49
Fraud scoring model – company specific	49
Order velocity monitoring	25
Positive lists	19
Customer order/Frequent flyer history	10

Purchase Device Tracing

Tool	%
IP geolocation information	26
Device "fingerprinting"	25

Multi-Airline Purchase History

Tool	%
Shared negative lists/hotlists	44
Fraud scoring model – third party	34

Base: Those using tool n=120

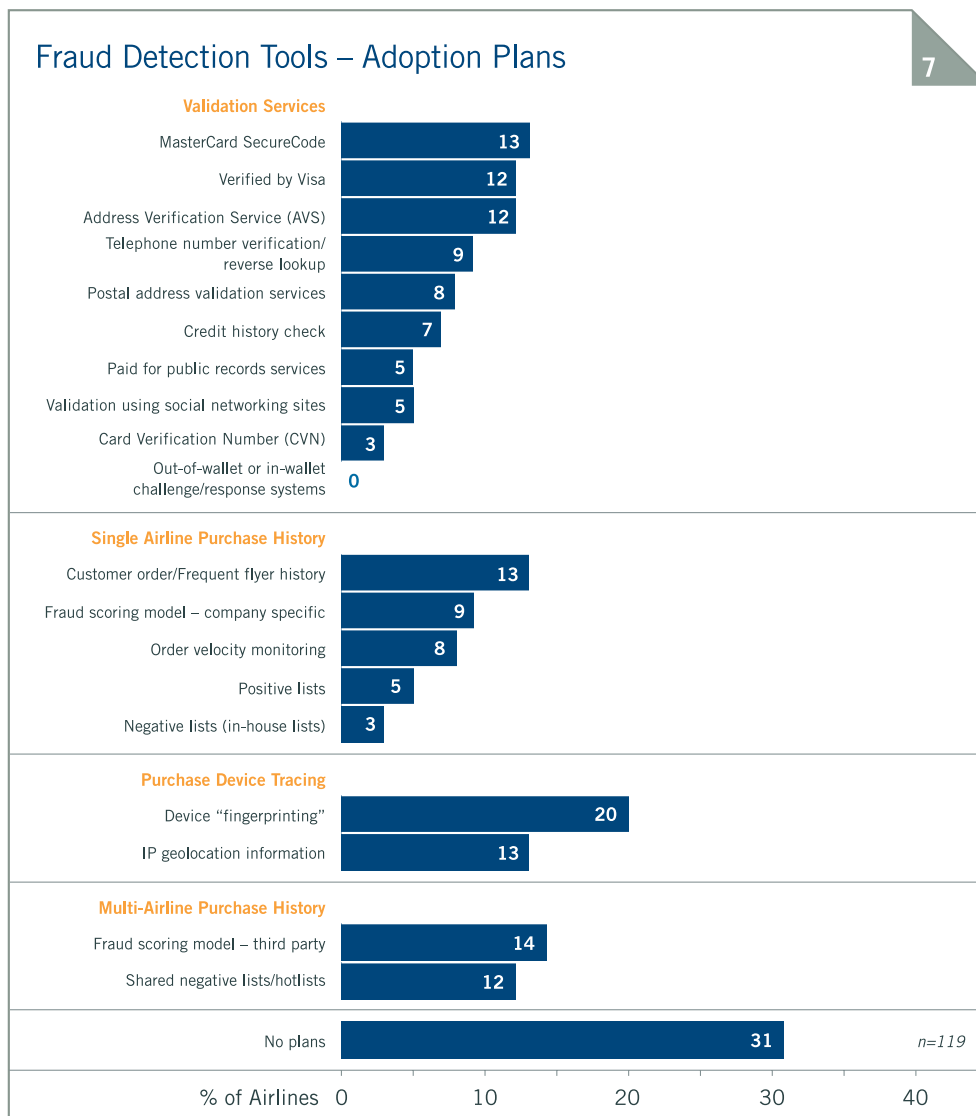% of Airlines 0 10 20 30 40 50 60 70

5

Planned Tool Adoption 2011

Device fingerprinting leads planned fraud detection methods for 2011, followed by implementation of a third-party fraud scoring model. One in five airlines surveyed reported they planned to implement device fingerprinting in 2011. Chart #7 shows the planned adoption across all fraud detection tools. Over two-thirds of airlines plan to adopt one or more new fraud detection tools in 2011.
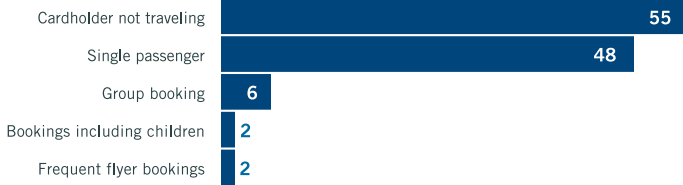
Common Fraud Risk Indicators

The survey asked airline fraud managers to select the six most common indicators of fraud risk. As expected, one-way flights, cardholder not traveling, and bookings made less than 12 hours prior to departure were high on the list of red flags (see Chart #8).
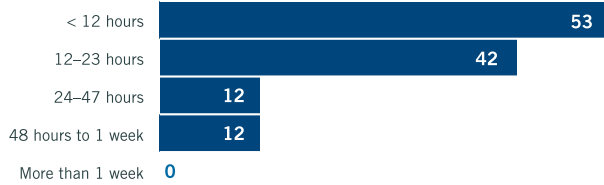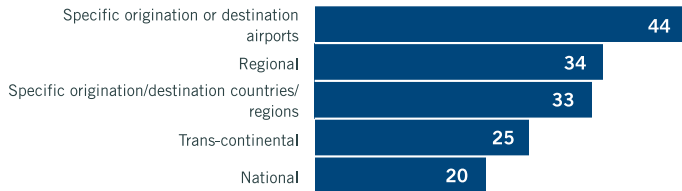
This year, airlines were also asked about specific origination/destination airports and countries. Both indicators ranked high, but flagging specific airports was higher. It's unlikely that a specific airport would be singled out without including other risk factors. For example, flights to a particular airport could be considered risky when coming from other specific airports, or perhaps even regions. This demonstrates the importance for airlines to examine full routing information in their fraud screening checks.

Fraud Detection Tools – Adoption Plans 7

Validation Services

MasterCard SecureCode	13
Verified by Visa	12
Address Verification Service (AVS)	12
Telephone number verification/reverse lookup	9
Postal address validation services	8
Credit history check	7
Paid for public records services	5
Validation using social networking sites	5
Card Verification Number (CVN)	3
Out-of-wallet or in-wallet challenge/response systems	0

Single Airline Purchase History

Customer order/Frequent flyer history	13
Fraud scoring model – company specific	9
Order velocity monitoring	8
Positive lists	5
Negative lists (in-house lists)	3

Purchase Device Tracing

Device "fingerprinting"	20
IP geolocation information	13

Multi-Airline Purchase History

Fraud scoring model – third party	14
Shared negative lists/hotlists	12

No plans	31

n=119

% of Airlines   0   10   20   30   40

Indicators of Fraudulent Bookings

8

Type of Booking

Cardholder not traveling	55
Single passenger	48
Group booking	6
Bookings including children	2
Frequent flyer bookings	2

Time Between Booking & Departure

< 12 hours	53
12–23 hours	42
24–47 hours	12
48 hours to 1 week	12
More than 1 week	0

Type of Itinerary

Specific origination or destination airports	44
Regional	34
Specific origination/destination countries/regions	33
Trans-continental	25
National	20

Type of Flight

One-way	56
Round trip	20
Multi-leg	8

Class of Service Booked

Economy	48
Business	21
Premium Economy	8
First	3
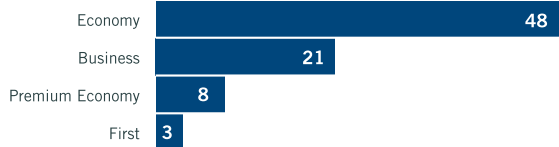
n=106

% of Airlines 0 10 20 30 40 50 60 70

BEST PRACTICE advice

No single tool can detect and prevent fraud, but the more data you have to analyze, the better able you are to detect fraud faster and more accurately. To improve fraud detection and combat fraud, focus on gathering as much data as possible on each booking, using an arsenal of tools together with proper fraud management practices and systems. Consider a layered defense using tools and data gathered in each of the four dimensions: validation services, single airline purchase history, purchase device tracing and multi-airline purchase history.

Stage 2: Manual Review

Booking → **Automated Screening** → **Manual Review** → **Accept / Reject** → **Fraud Claim Management** → Retained Revenue

Tuning and Management

Following the automated screening stage, questionable bookings typically enter a manual review stage, whereby a reviewer further investigates the booking and performs a risk assessment. During this process, additional information is collected to evaluate whether bookings should be accepted or rejected due to excessive fraud risk. In 2010, 80% of airlines reported manually reviewing their bookings for online payment fraud.

Manual Review Rates

For airlines that conduct manual review, approximately three out of every ten bookings are selected for further evaluation. Nearly two-thirds of airlines reported flagging up to 10% of bookings for manual review, while the remainder was spread between 10% and 100% of bookings (see Chart #9).

A considerable proportion, 14%, manually reviewed nearly every booking. For these airlines, there is significant opportunity to reduce costs and increase automation.
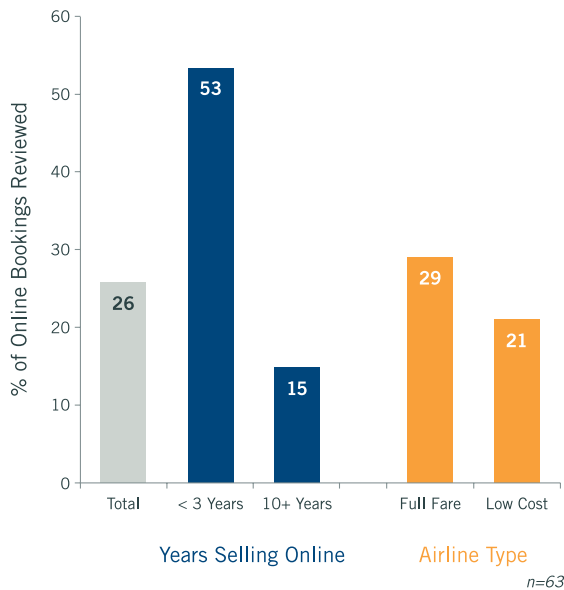
As Chart #10 highlights, airlines with more online experience manually review fewer bookings, which may be due to more experience in fighting online fraud, as well as more automated fraud prevention processes. Low cost carriers also had a lower review rate (21%) in comparison to both the average (26%) and to full fare carriers (29%). Airlines in Latin America reported employing the highest average number of staff involved in manual booking review, while those in Europe reported among the lowest.

Airlines expecting increased online sales will need to take at least one of the following actions: 1) divert more staff time to the booking review process; 2) increase staffing levels;

% of Airlines by Manual Review Level

9

% of Airlines

% Bookings Manually Reviewed	Value
< 10%	63
10% to 19%	10
20% to 29%	5
30% to 89%	8
90%+	14

n = 63
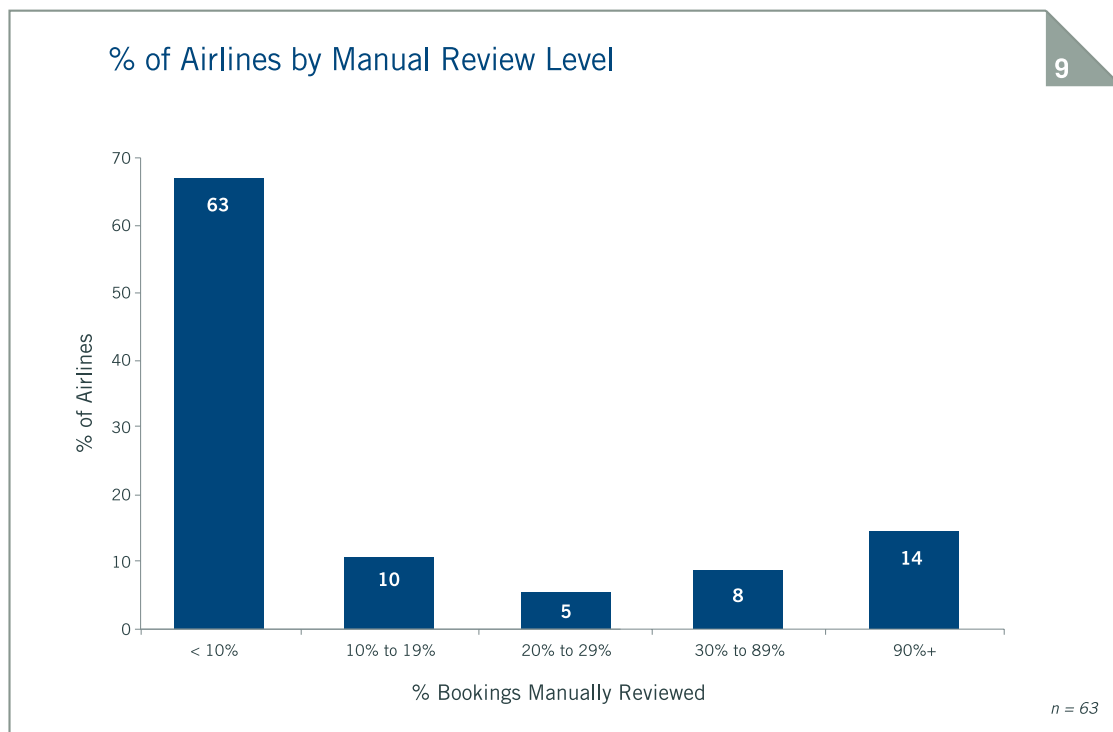
% of Online Bookings Manually Reviewed for Fraud

10

% of Online Bookings Reviewed

Total	26
< 3 Years	53
10+ Years	15
Full Fare	29
Low Cost	21

Years Selling Online   Airline Type

n=63

There are several actions airlines can take to optimize manual review processes. The first is to use a case management system which consolidates all booking-related information, minimizing time and effort around gathering and searching for data. The system should also allow customizable rules to be applied to address particular fraud patterns. Secondly, ensure that reviewers receive ongoing training in addition to a structured framework and procedural checklist to review a suspicious booking. Finally, apply the adage of what gets measured, gets improved. Statistics such as the time a booking is in queue before it is reviewed, and the average time each reviewer spends per booking, are vital to gauge the health of the process and to serve as a foundation for improvement.

3) allow more time to process bookings; or 4) improve the accuracy of initial automated sorting to make the subsequent review process more efficient.

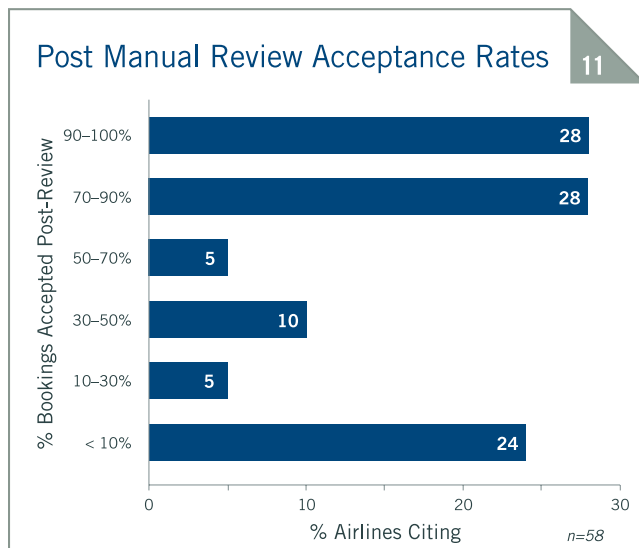## Reviewer Productivity and Final Booking Disposition

Airlines reported that each reviewer dispositions a median of 100 bookings per day for payment fraud. Automated screening and manual review ultimately result in booking acceptance or rejection. A relatively high percentage of bookings manually reviewed are ultimately accepted (see next section), highlighting the need for airlines to improve automated screening accuracy and thereby reduce the need for review. A look at booking reject and acceptance rates follows in Stage 3 of the pipeline review.

Stage 3: Order Dispositioning (Accept / Reject)

Booking → Automated Screening → Manual Review → Accept / Reject → Fraud Claim Management → Retained Revenue

Tuning and Management

Post-Review Booking Acceptance Rates

On average, 61% of bookings manually reviewed in 2010 were later accepted by airlines in the survey (see Chart #11). Yet 28% of airlines reported manually reviewing and later accepting nearly all suspected bookings. Over half of airlines in the survey still accept more than 70% of bookings that went to manual review, indicating that there is still opportunity for more efficiency in the automated screening process.

Post Manual Review Acceptance Rates   11

% Bookings Accepted Post-Review	% Airlines Citing
90–100%	28
70–90%	28
50–70%	5
30–50%	10
10–30%	5
< 10%	24

n=58

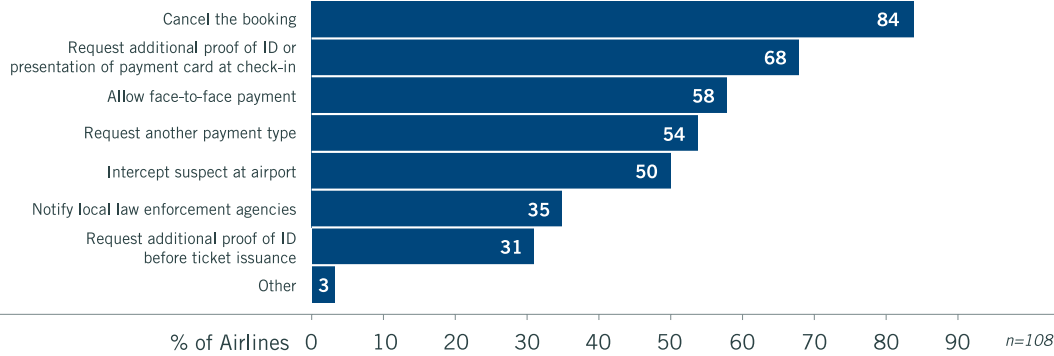## Overall Booking Rejection Rates

Booking rejection rates can reflect true fraud risk, or indicate "profit leaks" in terms of valid booking rejection or unnecessarily high rates of manual review. Rejection rates vary by years of online experience and type of carrier (see Chart #12). Full fare carriers have nearly three times the rejection rate of low cost carriers. In terms of booking rejection rates by region, Asia Pacific, Latin America, and the Middle East are among the highest, while North America and Europe are the lowest. Overall, the airlines surveyed rejected an average of 3.3% of online bookings, with over a quarter of airlines rejecting more than 5%.

Actions Taken on Suspicious Bookings

When a potentially fraudulent booking is identified, airlines take several actions depending upon their fraud management strategy. The most common action taken is simply to cancel the booking, as 84% of airlines reported in 2010. However, this action can lead to potential customer insult and revenue loss for those bookings that are not truly fraudulent or in cases where a genuine customer has unwittingly been sold a ticket purchased by fraudulent means. Airlines in the survey are taking several other steps to mitigate this risk (see Chart #13).

More than two-thirds of airlines request additional proof of identification or the payment card used for booking during check-in. While this method may help with revenue capture, it can also delay boarding and flight departure for both the passenger in question as well as other passengers. If the passenger is denied boarding, the airline will have limited recourse to re-sell seat inventory. Many airlines try to minimize the amount of fraud checking required at the airport, as any delays to flights departing caused by such checks can result in high fees to the airline from the airport authorities.

Average % of Online Bookings Declined Due to Suspicion of Fraud

12

Chart: % of Online Bookings Declined (y-axis 0–7)

- Total: 3.3
- < 3 Years: 6.8
- 3–4 Years: 2.8
- 5–6 Years: 4.4
- 7–9 Years: 2.1
- 10+ Years: 2.3
- Full Fare: 3.9
- Low Cost: 1.4

Years Selling Online   Airline Type
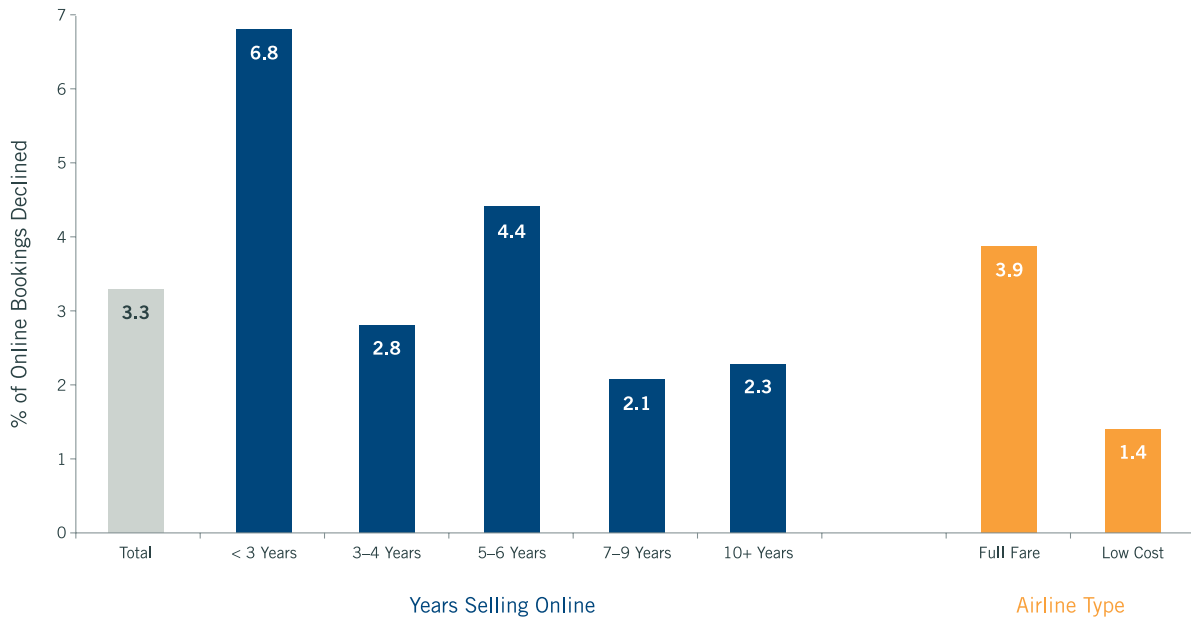
n=62

Actions Taken on Suspected Fraud Bookings

13

- Cancel the booking: 84
- Request additional proof of ID or presentation of payment card at check-in: 68
- Allow face-to-face payment: 58
- Request another payment type: 54
- Intercept suspect at airport: 50
- Notify local law enforcement agencies: 35
- Request additional proof of ID before ticket issuance: 31
- Other: 3

% of Airlines 0 10 20 30 40 50 60 70 80 90   *n=108*

BEST PRACTICE advice

Given that over 60% of manually reviewed bookings are ultimately accepted, consider fine-tuning the automated screening process to assess more transactions up front. This can reduce the workload for the review team, as well as limit the number of additional staff required as sales volume grows. Start by closely analyzing the bookings that go to manual review and are ultimately accepted, identifying the common attributes. Are there rules you can build on these attributes, to shift these bookings into the automated screening stage? The same approach can also be applied to bookings that are ultimately rejected. However, nearly 25% of airlines surveyed do not track fraud rates for online bookings that have been approved after manual review. Without this information, the systemic causes of fraud loss and process efficiencies between automated and manual review cannot be fully understood. Lastly, simply consider offering other payment options — only 54% of airlines surveyed requested another payment type as a means of substantiating a questionable booking.

Stage 4: Fraud Claim Management

Types of Fraudulent Bookings

Fraudulent bookings may take one of two paths back to airlines: through a chargeback or through a consumer credit request due to fraudulent use of their account. Chargebacks may incur fees from the bank or processor and require administration and management to challenge them. In this survey, airlines were asked to report on "friendly" fraud, which was defined as a customer who denied making the purchase, yet there is no other evidence of third-party fraud involvement.

Friendly Fraud

Over three-quarters of airlines surveyed indicated that the volume of friendly fraud had increased or remained the same in the preceding 12 months. This is consistent with results from non-travel merchants[3], where nearly two-thirds reported an increase in friendly fraud and also reported that on average, half of fraud claims consisted of consumer issued credit[4].

Fighting Chargebacks

The airlines' chargeback re-presentment rates reported in the survey generally follow a bi-modal distribution: with a generous portion fighting few chargebacks and another portion fighting nearly all (see Chart #14). In this survey a quarter of airlines re-presented nearly every fraud-coded chargeback.

Net Recovery Rate = **22%**

On average, airlines that fight chargebacks win **32%**

The average re-presentment rate is 49%. Airlines with more online experience were also less likely to re-present and win fraud-coded chargebacks, which may be due in part to difficulty extracting data from legacy systems in a timely manner or a lack of visibility within third-party systems.

Fraud Chargeback Re-Presentment Rates

The average chargeback win rate is 32%, which translates to an overall recovery of 22% of total chargebacks.

Methodology Note: Because of the wide variance in chargeback re-presentment practices, we calculated the net recovery rate for each airline participating in the survey, and then averaged the result, which came to 22%.

3. CyberSource 12th Annual Online Fraud Report (North America)
4. Ibid

Call Center Fraud

Nearly all airlines surveyed also supported sales through a call center. Call center fraud appears to be a growing issue among airlines, as over 40% of airlines perceived that call center fraud rates were about the same or higher than online fraud rates. In addition, nearly 40% of airlines also reported that the call center fraud rate was increasing in 2010. Airlines, like other online merchants, are generally less able to protect themselves from fraud in the call center channel due to the lack of applicability of many online fraud tools.

Fraud Rate Metrics

When reviewing the level and trend of online fraud loss, there are two key metrics on which to focus: 1) overall revenue lost as a percent of total online bookings; and 2) percent of accepted bookings which turn out to be fraudulent. It is important that airlines track key fraud metrics over time and evaluate performance relative to their peer group.

Note: This report provides benchmarks on total fraud loss rates for online sales via an airline's own website(s). Survey loss rates tend to be higher than those reported by banks and card schemes, because we have also included losses from other payment methods as well as credits or refunds issued to maintain customer goodwill. Fraud loss risk tolerances and booking rejection rates can vary significantly by airline.

Direct Revenue Loss Rates

In general, airlines with more years of online sales experience reported having a lower fraud rate than those with fewer. More experienced carriers tend to have lower fraud rates as they typically use more tools, have more refined fraud detection techniques, and may have more resources to manage online fraud. Survey results show that those with less than three years online sales experience use fewer tools (6.4 vs. 7.8) and have a fraud loss rate that is over three times higher than airlines with ten or more years of online sales experience (1.7% vs. 0.5%, respectively). Chart #15 shows the distribution of loss rates reported by airlines responding to the survey.
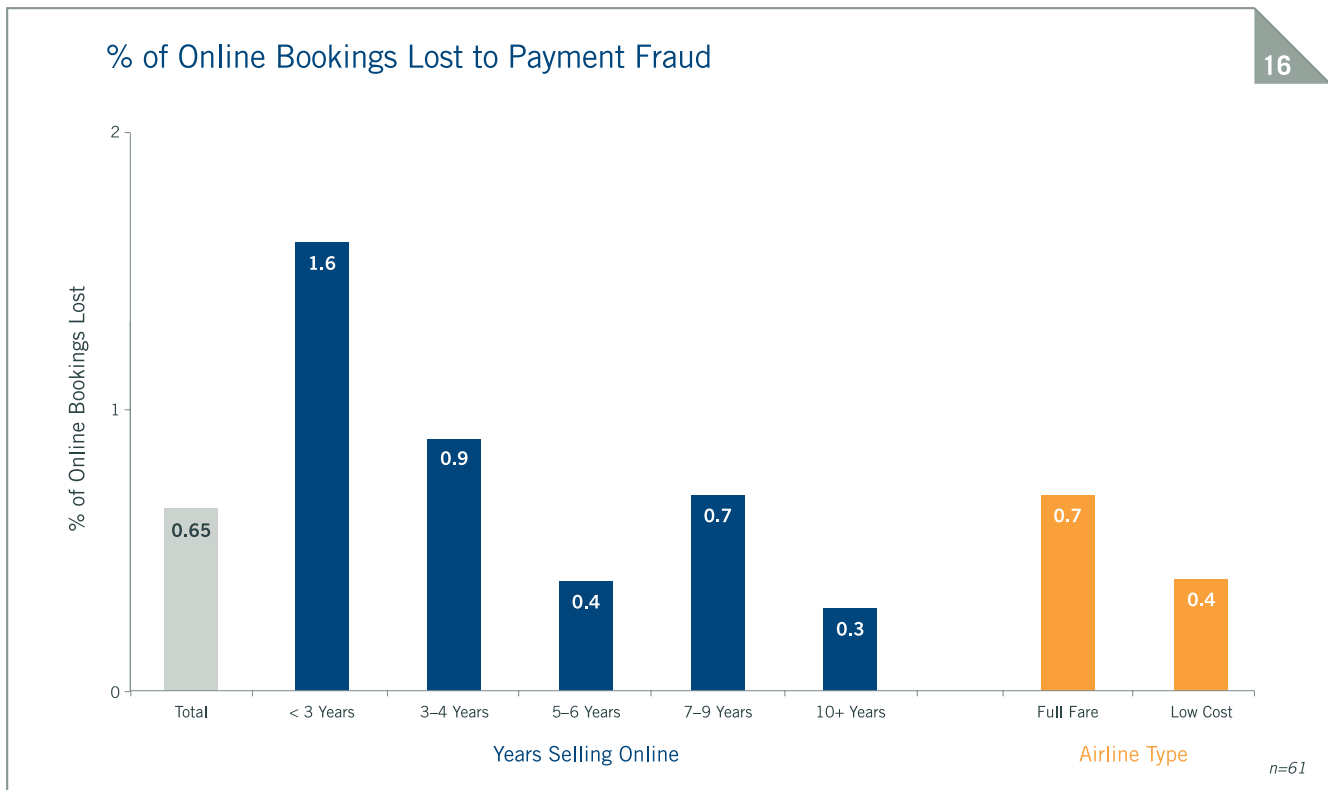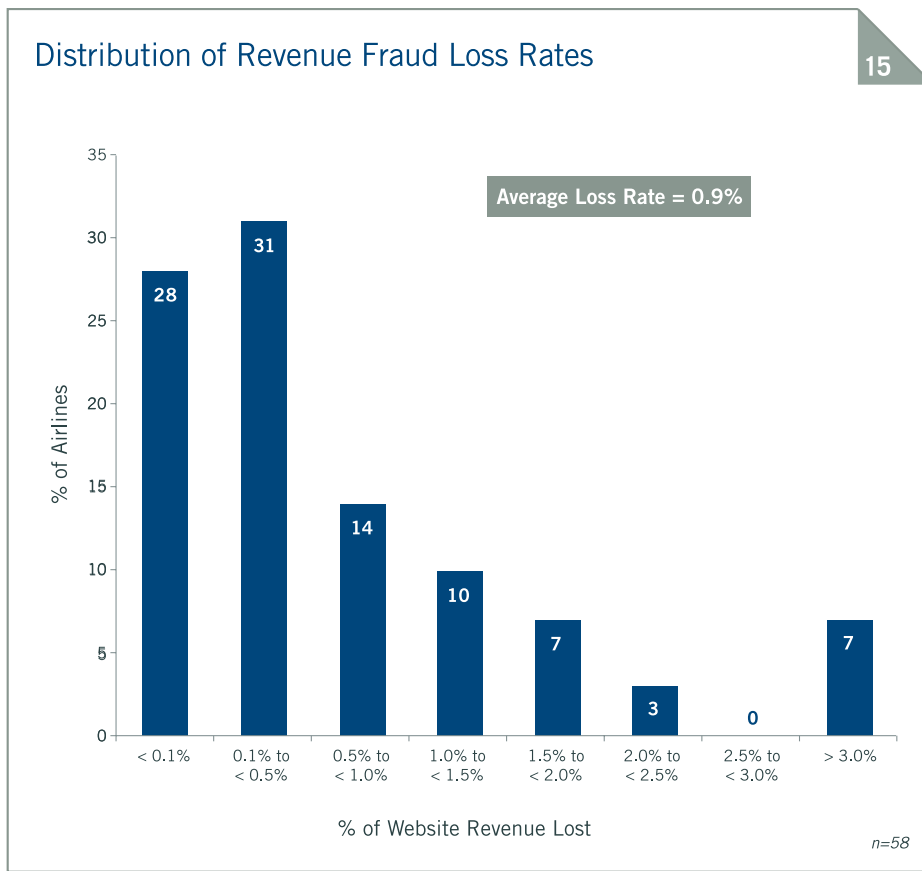
Fraud Rate for Accepted Bookings

The fraudulent booking rate is the number of accepted bookings that later turn out to be fraudulent, expressed as a percent of total bookings. In 2010, the fraudulent booking rate average was 0.65%, in comparison to 1.5% two years prior. Carriers in Latin America reported the highest fraudulent booking rate, while carriers based in most other regions averaged closer to the overall fraudulent booking rate of 0.65%. As airlines in Latin America also report a high post-manual review acceptance rate, this may indicate an opportunity to optimize manual review processes and provide additional training to their staff.

Figures for Chart #16 include both chargebacks and credits issued directly by the airline in response to fraud claims.

BEST PRACTICE
advice

Although it may not make sense in every instance, consider challenging more of your chargebacks. To successfully dispute chargebacks, gather as much data as possible as part of the whole transaction process, to corroborate that the person making the booking was legitimate. In addition to accessing a wide range of information about the chargeback, such as booking data and payment specifics, any other information—such as proof that the cardholder flew on the purchased ticket—is helpful and relevant. An efficient re-presentment process can help enhance profitability and reduce fraud loss.

Distribution of Revenue Fraud Loss Rates

15

Average Loss Rate = 0.9%

% of Airlines

% of Website Revenue Lost

< 0.1% : 28
0.1% to < 0.5% : 31
0.5% to < 1.0% : 14
1.0% to < 1.5% : 10
1.5% to < 2.0% : 7
2.0% to < 2.5% : 3
2.5% to < 3.0% : 0
> 3.0% : 7

n=58

% of Online Bookings Lost to Payment Fraud

16

% of Online Bookings Lost

Total : 0.65
< 3 Years : 1.6
3–4 Years : 0.9
5–6 Years : 0.4
7–9 Years : 0.7
10+ Years : 0.3
Full Fare : 0.7
Low Cost : 0.4

Years Selling Online   Airline Type

n=61

14

Tuning & Management

Booking → Automated Screening → Manual Review → Accept / Reject → Fraud Claim Management → Retained Revenue

Tuning and Management

Fraud review staffing can take up a sizable portion of fraud management budgets, as manual review is labor-intensive and costly. Of the airlines surveyed, only 11% reported they would be adding to their fraud review staffing in 2011 (see Chart #17).

In total, 82% of airlines indicated that one to five staff members were involved in manual review, with an average of 4.7 staff members. Airlines with less than three years and those with more than ten years of online sales experience had more review staff than average. Airlines with less experience are less likely to have automated fraud tools and processes in place, while those with more experience may have enough booking volume to support more staff for manual review.

Although 92% of airlines expected an increase in online sales in 2011, 67% expected no change in manual review staffing.

This may reflect the lag in staff buildup and a desire to extend worker productivity while the economy continues to recover. However, without an optimized fraud management process in place, scalability may become an issue. The

Manual Review Staffing Levels 2011 Plans

17

Add Staff
11%

Reduce Staff
22%

No Change in Staffing
67%
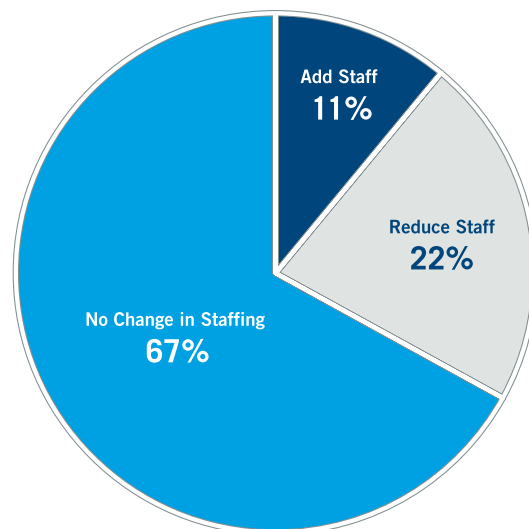
n=54

BEST PRACTICE
advice

Consider implementing fraud tools and strategies through a fraud management portal. Typically, portals provide access to a rules engine where business managers can create screening criteria based on information derived from a portfolio of verification and validation services. With a flexible rules system, business managers can screen different profiles based on payment type, product type, and other market-specific criteria. In addition, look for those portals where the case management systems are integrated with accompanying enhancements to streamline workflow. Reducing the manual review workload and increasing reviewer productivity are key to maximizing profit while keeping overall fraud management costs in line. An excellent place to start is by improving the automated detection of risky bookings to reduce manual review volumes.

review team will come under pressure to review more bookings within a limited timeframe, and without the right tools and processes in place, bookings in queue will become a growing concern. As budgets come under increasing pressure, airlines will need to re-double their efforts to automate more of the fraud management process, while keeping valid booking conversion high and fraud loss low.

Conclusion

To provide an overall assessment and basis of comparison, we took a snapshot of average airline performance across three key performance indicators (KPIs): manual review rate, percent of bookings declined, and percent of revenue lost due to online payment fraud. In summary, although the survey results still show a wide range of fraud management practices, airlines showed overall improvement in reducing online payment fraud by 31% (0.9% vs. 1.3% two years prior).
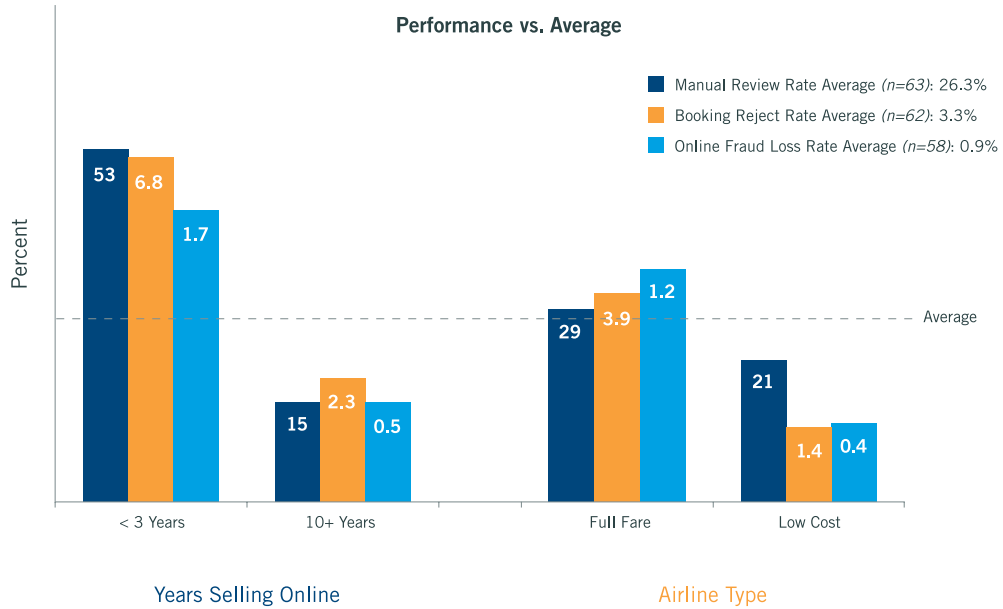
KPIs vary by years of online experience and business model (see Chart #18). Airlines with more experience tend to fare better, if only because they've been on the front lines longer and typically have more tools and fraud management processes in place. Low cost carriers seem to have tightened their fraud management processes, yet continue to have above average rates of post-review acceptance, which may point to a need for further screening optimization.

KPIs also vary significantly by region (see Chart #19). Regional differences are often attributable to not only the type of airline, online fraud management and online experience, but also due to the unique fraud challenges presented in those regions.

Each airline faces a unique set of business goals, fraud tolerance and risks. For that reason, a structured and tailored approach to fraud management is critical. Airlines must weigh the trade-offs among review costs, booking rejection, and fraud losses, and constantly fine-tune their overall processes to optimize all three.
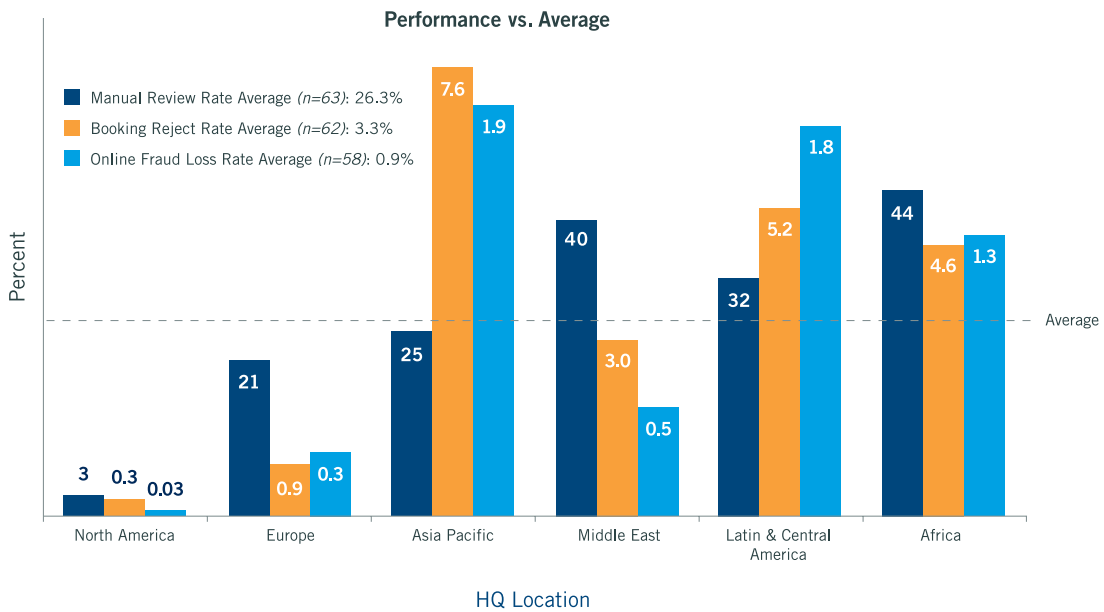
KPI Relative Performance by Experience & Type

18

Performance vs. Average

■ Manual Review Rate Average *(n=63)*: 26.3%
■ Booking Reject Rate Average *(n=62)*: 3.3%
■ Online Fraud Loss Rate Average *(n=58)*: 0.9%

Percent

< 3 Years: 53 | 6.8 | 1.7
10+ Years: 15 | 2.3 | 0.5
Full Fare: 29 | 3.9 | 1.2
Low Cost: 21 | 1.4 | 0.4

Average

Years Selling Online — **Airline Type**

KPI Relative Performance by HQ Location

19

Performance vs. Average

■ Manual Review Rate Average *(n=63)*: 26.3%
■ Booking Reject Rate Average *(n=62)*: 3.3%
■ Online Fraud Loss Rate Average *(n=58)*: 0.9%

Percent

North America: 3 | 0.3 | 0.03
Europe: 21 | 0.9 | 0.3
Asia Pacific: 25 | 7.6 | 1.9
Middle East: 40 | 3.0 | 0.5
Latin & Central America: 32 | 5.2 | 1.8
Africa: 44 | 4.6 | 1.3

Average

HQ Location

Resources & Solutions

To find information on CyberSource's industry-leading fraud management solutions, self-paced webinars, and other whitepapers on electronic payment management, visit our online Resource Centers:

Americas:
Visit www.cybersource.com. For sales assistance, call +1 650 965 6000 or email sales@cybersource.com

Europe | Middle East | Africa:
Visit www.cybersource.co.uk. For sales assistance, call +44 (0) 118 929 4840 or email uk@cybersource.com

Asia Pacific:
For sales assistance, call +65 6499 2000 or email asia@cybersource.com

Japan:
Visit www.cybersource.co.jp. For sales assistance, call +81 3 5774 7733 or email sales@cybersource.co.jp

CyberSource Fraud Management Solutions

CyberSource's industry-leading risk management solutions enable airlines to detect fraud sooner and more accurately, as well as streamline fraud management operations. With a hosted fraud management system and managed risk services that can supplement or manage complete portions of your review process, CyberSource provides flexible and powerful options that best meet your business needs.

CyberSource Decision Manager: Rule Console and Fraud Detectors

Having more data enables you to gain more insightful correlations to detect sophisticated fraud. Decision Manager is a hosted system providing access to a full range of data generated from global fraud detectors, cross-merchant and cross-industry correlations, truth data and more. Decision Manager comes with a business rule console that controls automated screening and case routing, an advanced case management system, and reporting and analytics.

Automatically screen more bookings up front, while providing your review team with access to fraud detectors and customized rules to help them review more bookings, faster and more accurately.

- Data Correlation Engine: correlates inbound booking data to over 200 real-time tests — including device information, a gigantic database of global cross-merchant transaction histories, and your own data to reveal even the subtlest of fraud anomalies.

- Business User Rule Console: enables your fraud analysts to create and customize rules without IT intervention, for faster, more accurate response to fraud attacks.

- Custom Data: data imported from your systems to better screen for fraud, including names of travelers, routes, frequent flyer numbers, etc.

- Case Management System: a workflow-savvy interface that consolidates information on bookings for faster review, with automated queue management that can prioritize cases by flight departure times. Includes automated case routing based on established rules, booking profiles, consolidated data review, and built-in callouts to validation services.

- Analytics: reporting and analytics to provide more visibility into your rule, reviewer, and overall fraud management process performance.

Payer Authentication
Provides the online guarantees offered by Verified by Visa and MasterCard SecureCode.

Managed Services
CyberSource Managed Services enables you to scale your expertise and capacity without adding fixed headcount. Our staff of fraud analysts, review and chargeback experts stand ready to back your team, or even manage complete portions of your operation. All of our services are backed by business performance guarantees.

- Performance Monitoring supports your team with fraud experts for help with configuring rules and detectors, and monitoring process performance.

- Screening Management includes our Performance Monitoring service, plus our expert review staff to manage manual review per your policies.

CyberSource Payment Management Solutions

In addition to our fraud management solutions, CyberSource offers a comprehensive portfolio of modular services and tools to help your airline manage your entire payment pipeline to optimize sales results. All are available via one connection to our web-based services.

Global Payment Acceptance

Accept payments worldwide using a merchant account from your preferred provider: worldwide credit and debit cards, regional cards, direct debit, bank transfers, electronic checks and other payment types such as Bill Me Later and UATP. CyberSource also provides professional services to help you integrate payment with front-end and back-office systems.

- Processing Management: CyberSource processes your payments in our high availability datacenters located in the U.S., Europe, and Japan. All datacenters are certified PCI-compliant and include sophisticated processing management logic to help prevent payment failures and rate downgrades.

- Collection & Reconciliation: a full array of online and exportable payment reporting capability is available to streamline reconciliation activity. Further, systems can be installed to automate up to 90% of the tasks associated with payment reconciliation and chargeback re-presentment.

Payment Security

Remove payment data from your network. A great way to streamline PCI compliance and mitigate security risk.

- Payment Tokenization and Hosted Payment Acceptance Services: enables you to process payments without storing or even transmitting payment data.

- Payment System Centralization: our team of experts will help you consolidate multiple payment systems into a single, easy to manage system. Link legacy systems/GDS to web-based services for rapid service expansion. Optionally, CyberSource will also host, support and manage these centralized payment systems in our secure datacenters.

Professional Services

CyberSource maintains a team of experienced payment consultants with proven airline integration expertise. Our client services team is additionally available to help you monitor, tune, or fully outsource portions of your payment operations.
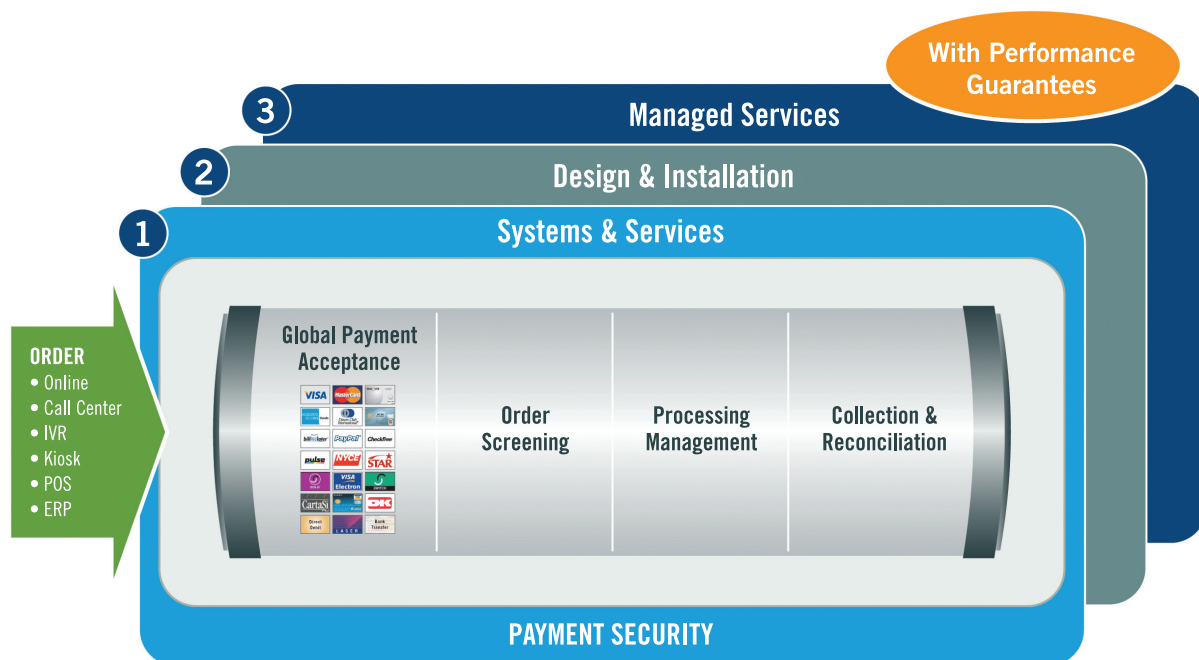
About CyberSource

CyberSource, a wholly owned subsidiary of Visa Inc., is a payment management company. Over 330,000 businesses worldwide use CyberSource and Authorize.Net brand solutions to process online payments, streamline fraud management, and simplify payment security. The company is headquartered in Mountain View, California with international offices in Reading, U.K.; Singapore; and Tokyo. CyberSource operates in Europe under agreement with Visa Europe.

About Airline Information

Airline Information is an established innovator in commercial aviation management conferences and publishing. Over 200 airlines regularly attend Airline Information conferences and forums worldwide. The firm provides airline professionals and industry suppliers with free high-quality online publications as well as premium guidebooks and management consultation in payments, loyalty, CRM, eCommerce, and ancillary revenue development. For more information please visit: http://www.airlineinformation.org.

CyberSource®

the power of payment