

CyberSource®
the power of payment



Airline Online
Fraud Report 

Online payment fraud
practices & benchmarks

2009 Edition

In association with  AirlineInformation

Report & Survey Methodology

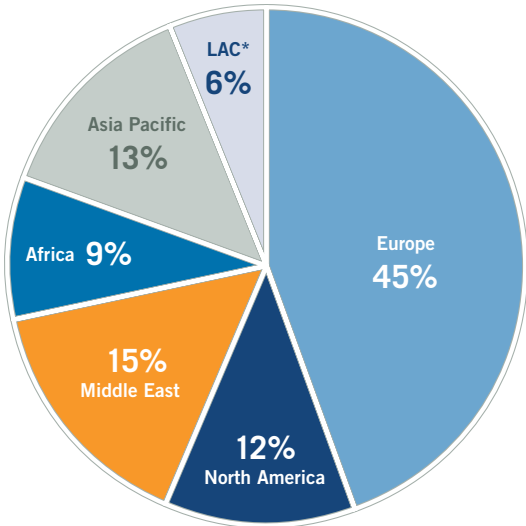
The CyberSource Airline Online Fraud Report, developed in association with Airline Information, is based on a survey of airlines from across of the globe, representing an estimated 25 percent of total worldwide online sales. Decision makers who participated in this survey were either ultimately responsible for, or had significant influence on, fraud management policies and decisions for their carrier.

Online selling experience levels range from airlines in their first year of online transactions to over nine years' experience selling via the web (see chart #1). Airlines participating in the survey ranged in size from less than \$500 million¹ in total annual sales to over \$10 billion. Airlines that took the survey reported online sales totaling \$40 billion in 2008.

The survey was conducted via online questionnaire by Mindwave Research, with additional telephone interviews conducted by Vanson Bourne Ltd. 99 participants completed the survey between December 1, 2008 and January 15, 2009.

Summary of Participants' Profiles

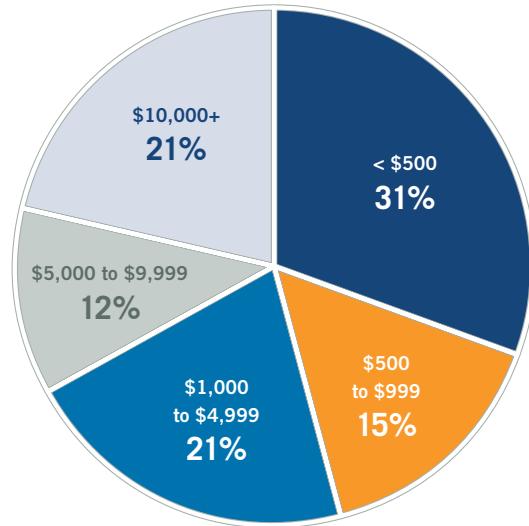
Airline HQ Location



*Latin America & the Caribbean

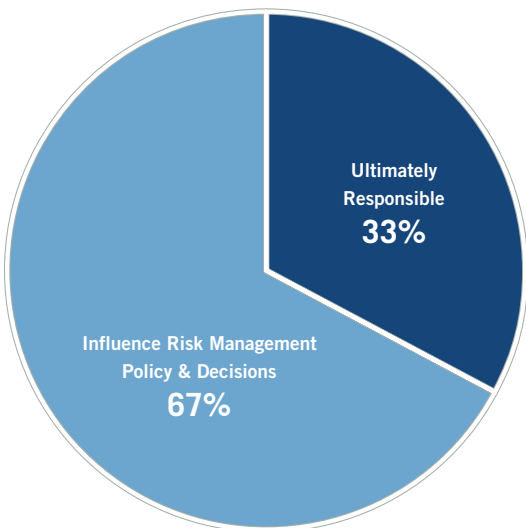
n=99

Annual Worldwide Revenue (USD Millions)



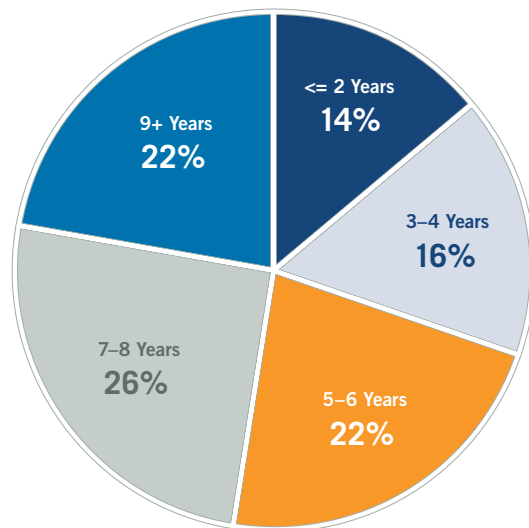
n=85

Risk Management Responsibility



n=99

Duration of Online Selling



n=98

Table of Contents

EXECUTIVE SUMMARY	1
STAGE 1: ORDER SCREENING	3
Fraud Detection Tools	3
Planned Tool Adoption 2009	6
Common Fraud Risk Indicators	6
STAGE 2: MANUAL REVIEW	8
Manual Review Rates	8
Reviewer Productivity	9
Final Booking Disposition	9
STAGE 3: ORDER DISPOSITIONING (ACCEPT/REJECT)	10
Post-Review Booking Acceptance Rates	10
Overall Booking Rejection Rates	10
Actions Taken on Suspicious Bookings	10
STAGE 4: FRAUD CLAIM MANAGEMENT	12
Fighting Chargebacks	12
Fraud Rate Metrics	13
Direct Revenue Loss Rates	13
Fraud Rate for Accepted Bookings	13
TUNING & MANAGEMENT	15
CONCLUSION	16
RESOURCES & SOLUTIONS	18

Executive Summary

Many airlines have been online sales pioneers. In this survey, airlines report one-third of their booking revenues come from the online sales channel, which is more than three times higher than the average for most non-travel companies selling online.

The online channel enables airlines to cost-effectively reach customers, but being on the front line of eCommerce presents additional challenges: managing online payment fraud, avoiding the rejection of valid bookings, and scaling fraud management to support online sales growth. The survey results show that while some airlines do a good job managing online fraud, performance varies widely by type of airline, geography and experience.

In this highly competitive industry, maximizing revenues while controlling costs is critical to long term success. To better understand the impact of payment fraud for airlines, CyberSource commissioned this survey. The study builds on the ten years of research that CyberSource has in benchmarking fraud trends experienced by online merchants.

Overview

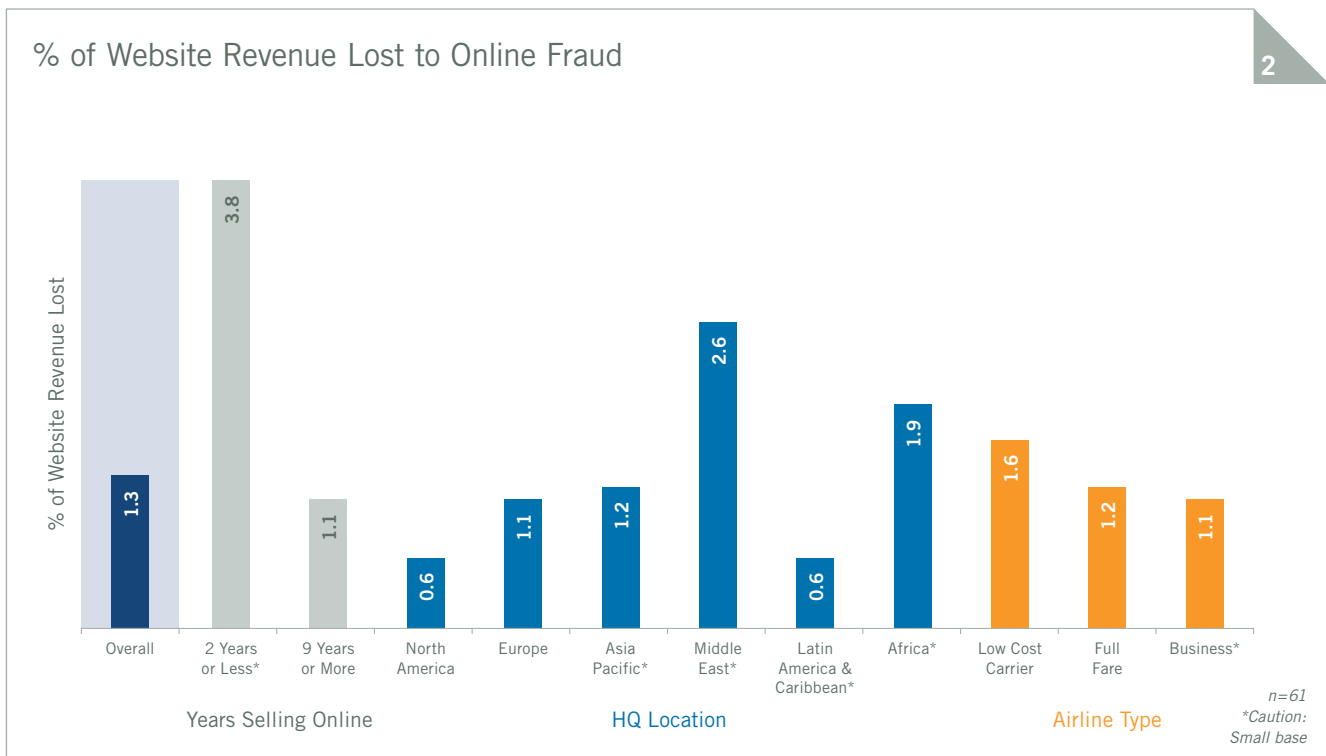
In 2008, airlines lost an estimated \$1.4 billion² in revenues to fraudulent online bookings made on their own websites. This represents approximately 0.9 percent of total worldwide online airline ticket sales. The average revenue loss rate on airline websites was 1.3 percent (see chart #2). This may seem high, but it is similar to the loss rates we have measured over the last few years among non-travel merchants selling online in North America.

Based on how we asked about revenue loss in the survey, the fraud losses reported include losses for all payment methods, in addition to 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 tend to have lower fraud rates and 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 we see by non-travel online merchants. These credits may also be issued by a different department in the airline, which may not be responsible for chargebacks or merchant account management.

The overall average loss of 1.3 percent of website booking revenues represents a range of loss experience among airlines surveyed. Half of the airlines surveyed reported website revenue fraud loss rates of less than 0.7 percent.

Fraud loss rates also vary widely by region. North American-based carriers reported the lowest loss rates, while those in the Middle East were four times higher. By airline type, low cost carriers reported the highest average fraud loss rate, while business class airlines reported one-third lower average loss rates. As one might expect, the highest average fraud losses were reported by airlines with two or fewer years' experience selling online. Their average fraud loss rate was over three times higher than airlines that have been selling online for nine or more years.



2. Estimated global losses were calculated by applying regional fraud loss rates from the survey to estimated regional online market sizes, then summing the regional losses in order to produce the worldwide estimate.

Key Fraud Metrics

There are other metrics beyond fraud loss rates to consider. These include the percent of website bookings which airlines reject due to suspicion of fraud, as well as the share of bookings that require additional manual review and verification before accepting or rejecting.

Airlines reported that for every fraudulent website booking, they rejected 1.9 additional bookings, on average, due to suspicion of fraud. The percent of total website bookings rejected due to suspicion of fraud also varies widely by type of airline, geography and online selling experience. Average rejection rates range from 0.8 percent to 8.4 percent, depending on geographic region. Business class airlines have the highest average rejection rate, while low cost carriers have the lowest.

On average, the survey results show that 30 percent of online bookings require additional manual review and verification. However, the level of automation and share of bookings reviewed also varies greatly, ranging from three percent for some regions to as high as 81 percent for others. Airlines surveyed report using an average of 5.8 tools to help detect online payment fraud. The average number of tools used ranges from a low of 4.7 for airlines based in Africa to 7.5 for North American carriers.

One-Third of Fraud Losses are Recoverable

Airlines report that they win almost half of the fraud chargebacks they re-present, resulting in an average net recovery of 32 percent of initial fraud chargeback claims. However, one-third of airlines surveyed report that they challenge fewer than ten percent of initial fraud claims, while 39 percent challenge 70 percent 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 order rejection and fraud rates as low as possible, to maximize sales and profits.

Total Pipeline View

Airlines that focus solely on managing chargebacks may not be seeing the complete financial picture. Online payment fraud impacts profits from eCommerce sales in multiple ways. In addition to direct revenue losses, consider the additional costs of rejecting valid bookings, staffing manual review teams, administration of fraud claims, as well as challenges associated with business scalability. 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 association limits), an end-to-end view is required to arrive at the best possible financial outcome.

In 2008, “profit leaks” in the Risk Management Pipeline™ impacted, on average, one-third 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



Stage 1: Order Screening

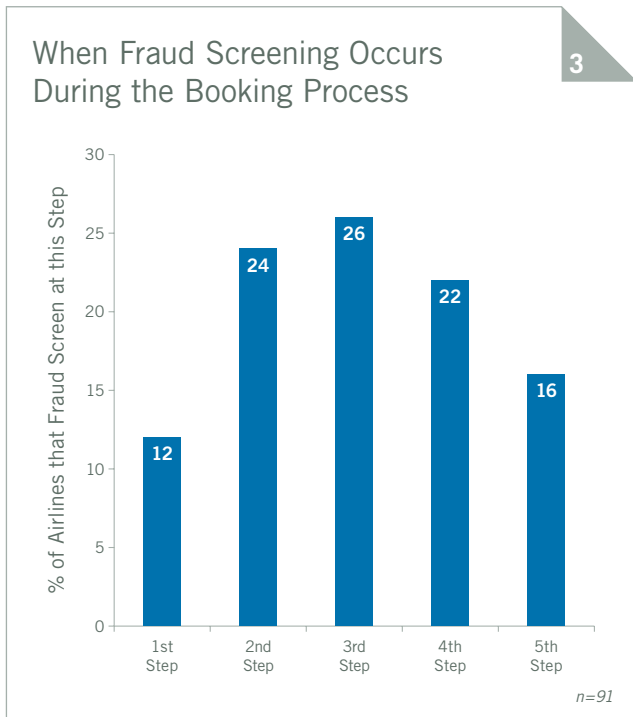


Fraud Detection Tools

We define detection tools as those used to identify the probability of risk associated with a transaction, or to validate the identity of the purchaser. A wide variety of tools is available to help airlines evaluate incoming bookings for potential fraud. These tools cut across four dimensions of fraud detection: global validation services, single airline purchase history, multi-airline purchase history, and purchase device tracing. Test results from these detection tools are then interpreted by humans or rules systems to determine if a transaction should be accepted, rejected or reviewed.

Airlines handling large online booking volumes typically employ an initial automated evaluation to determine if an incoming booking might represent a fraud risk. Based on the results of this initial risk screening, bookings are then assigned one of three statuses: accept, decline or suspend for further review.

To better understand when fraud screening takes place, we asked airlines to “rank order” five key steps in the booking process. The steps offered for ranking were: booking generated, payment authorization, booking screened for fraud, ticket issuance, and payment settlement. As chart #3 shows, practices vary widely in terms of when fraud screening occurs.

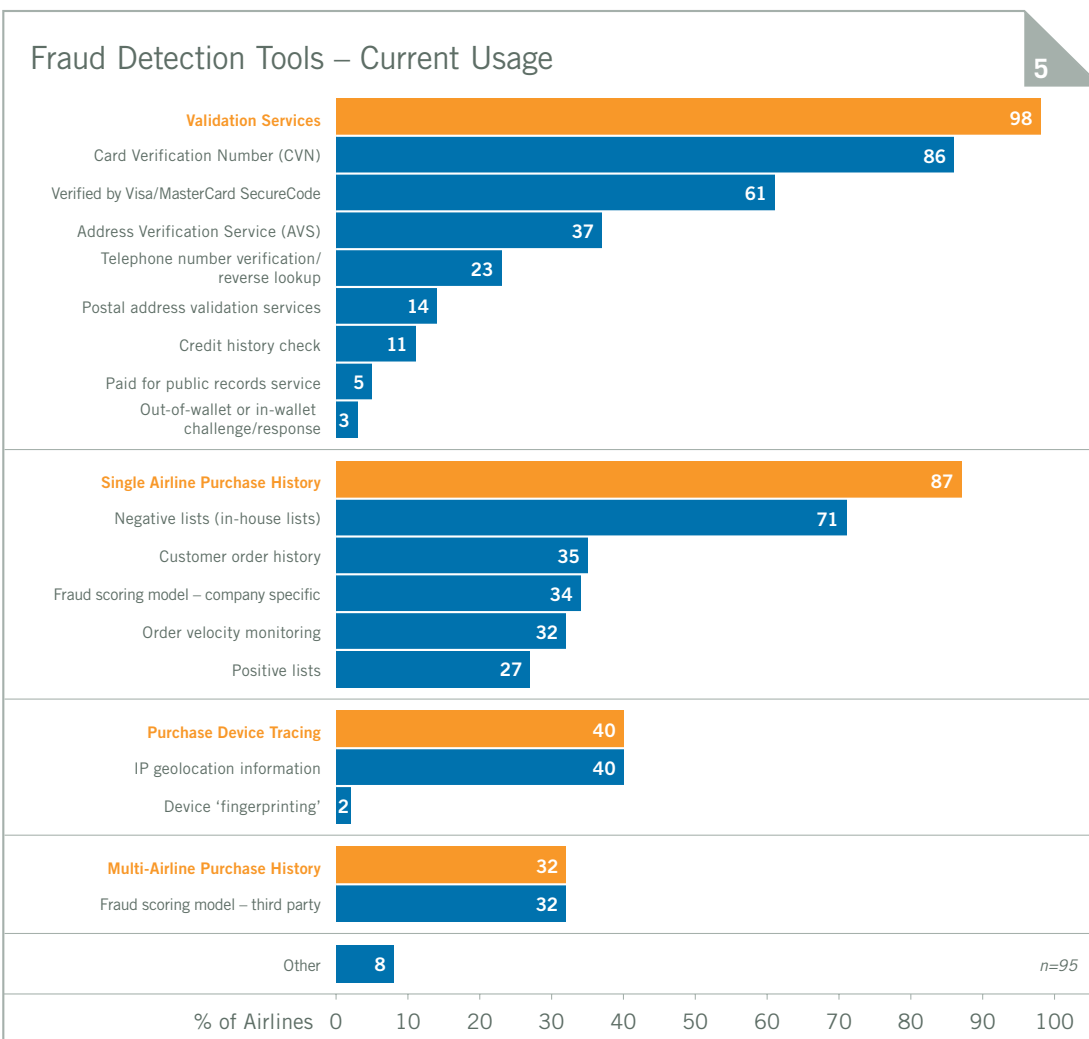
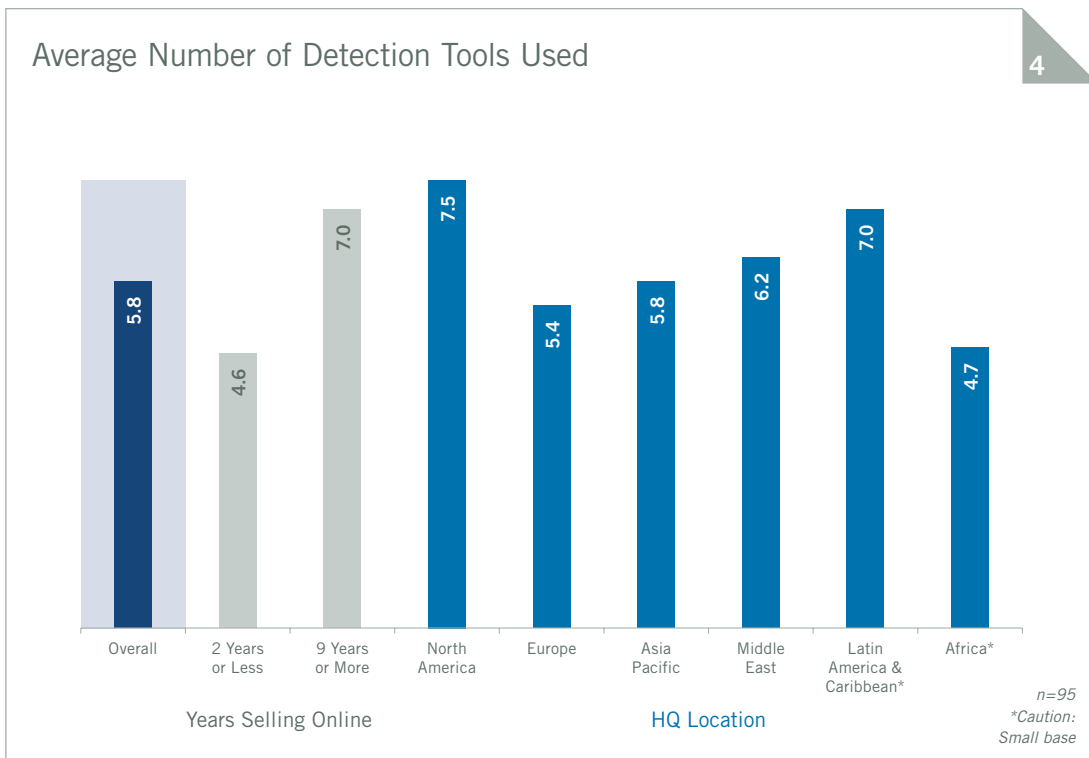


While European and Middle Eastern airlines tend to undertake fraud screening earlier in the online booking and payment process, North American and Asian airlines tend to do it later. These differences may be attributable to the global distribution systems used in different regions and who handles the payment processing.

On average, airlines report using 5.8 fraud detection tools to screen online bookings. This compares to 4.7 for non-airline industries³. Chart #4 shows that North American and Latin American airlines report using the largest number of fraud detection tools. However, they do not achieve the same fraud management results despite similar tool use (see Stage 4 discussion). Airlines selling online for two years or less have the lowest average tool use and have higher fraud losses than carriers with more eCommerce experience. In addition, fraud detection tool use also varies by type of airline.

The most popular tools used to assess online booking fraud risk are shown in chart #5. Overall, 98 percent of airlines use one or more validation services, which are often provided by the card associations to help authenticate cards and card holders.

3. CyberSource 10th Annual Online Fraud Report (North America)



Card Verification Number (CVN; also known as CVV2 for Visa, CVC2 for MasterCard, CID for American Express and Discover) is the most commonly used detection tool. The purpose of CVN in a card-not-present transaction is to attempt to verify that the person booking the flight has the actual card in his or her possession. Requesting the CVN during an online purchase can add a measure of security to the transaction. However, CVNs can be obtained by fraudsters just as easily as credit card numbers.

Airline proprietary negative lists are the second most commonly utilized tool, with 71 percent of airlines reporting their use. Interestingly, positive lists and customer order history are used less frequently, which seems counter-intuitive, as airlines have order histories and frequent flyer programs that could provide rich data on the purchaser.

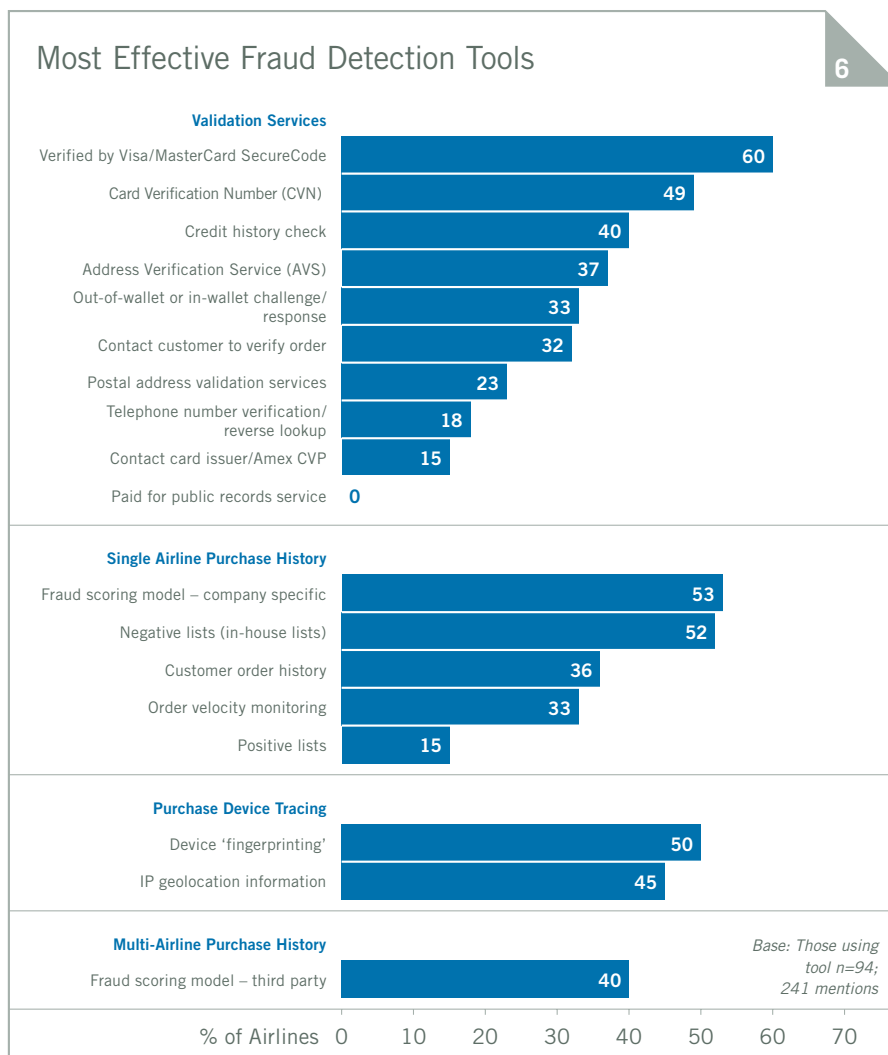
The card association payer authentication services (e.g. Verified by Visa, MasterCard SecureCode) are the third most commonly used tool. This could, in part, be due to MasterCard’s requirement that any organization wishing to accept Maestro card transactions online must be SecureCode enabled. The favorable discount rates offered by the card associations for payer authentication may also play a role.

Airlines were asked to identify the three most effective tools they use. To eliminate bias toward the more commonly used tools, we normalized the data by looking at the percent of airlines using a particular tool, citing that tool as one of their top three choices. Chart #6 shows the results of this analysis.

Card association payer authentication systems received the highest rating as being an effective tool by airlines that use this option, perhaps because they still receive a liability shift if the authentication services are used correctly – even for cards not enrolled in payer authentication⁴. However, other factors may also be at play.

Analysis of the survey data shows that use of payer authentication systems is highly correlated with the total number of fraud management tools used and years of online selling experience. We believe that fraudsters who see that an airline has implemented payer authentication move on to easier targets, because they most likely view this as an indicator that an airline has better fraud management systems and practices in place.

Several other tools are mentioned as very effective by half their users – custom fraud scoring models, negative lists, device fingerprinting and CVNs round out the list of tools considered to be most effective.



4. Rules for liability shift are more favorable outside the United States, and may not require card enrollment.

Planned Tool Adoption 2009

Multi-merchant third-party fraud scoring models rank highest on “plan to buy” lists

40 percent of airlines surveyed said they expected to implement a third-party risk scoring model in 2009. Such models, using online and offline transaction data across multiple airlines, can be highly effective in detecting new fraud patterns and risks that a single airline may not have encountered. Chart #7 shows the planned adoption across all fraud detection tools. 77 percent of airlines plan to adopt one or more new fraud detection tools in 2009.

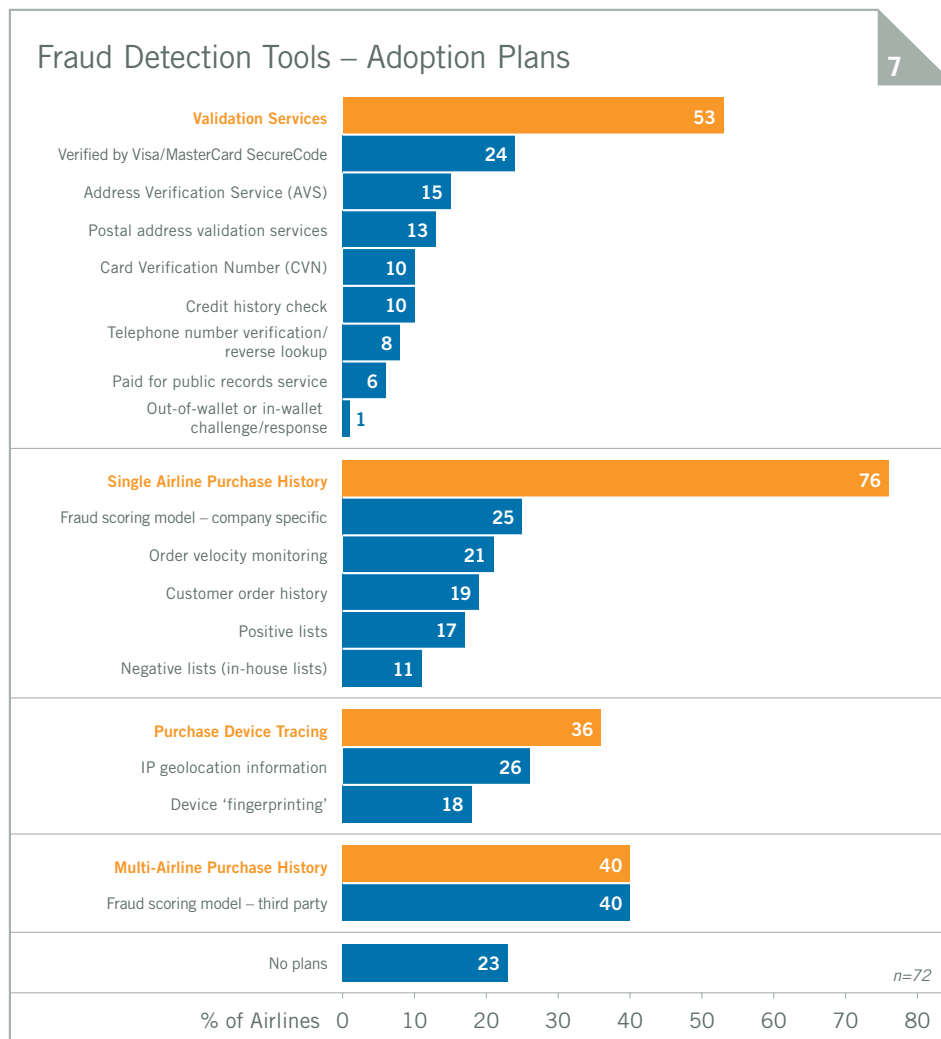
Common Fraud Risk Indicators

The survey asked airline fraud managers to note the six most common indicators of fraud risk. The results confirm what is well known in the industry – the highest risk indicators involve bookings where the passenger and the payer are not the same

person; the time between booking and flight departure is less than 24 hours; and the booking is for a one-way journey.

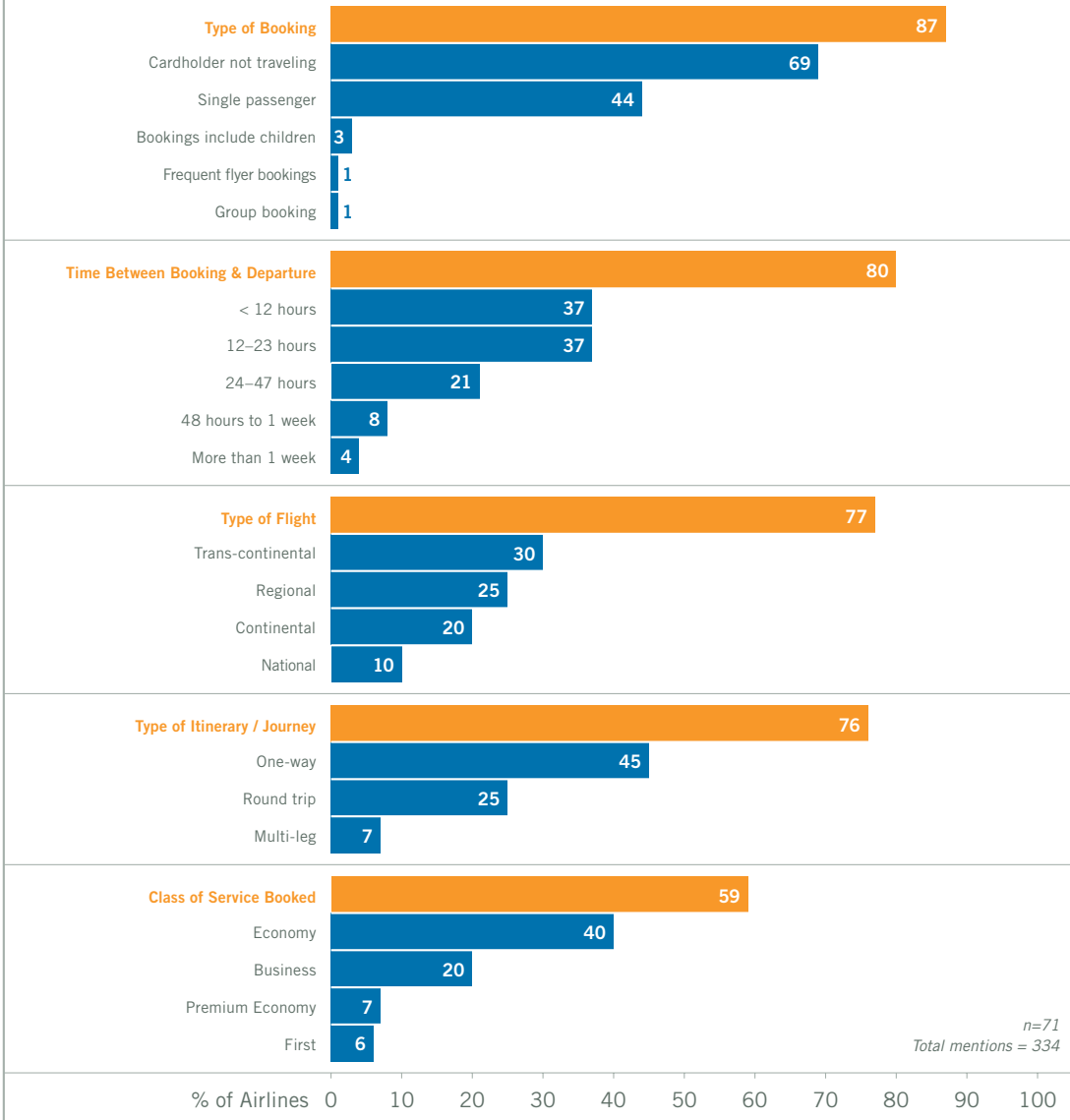
As a general rule, the most successful fraudsters are expert at making online transactions appear as normal as possible – attempting to camouflage fraud as valid transactions. High order volumes help fraudsters hide in the transaction stream, so it is not surprising that economy class tickets are listed as one of the six common risk indicators instead of more expensive classes of service.

While one-way bookings are a common fraud indicator, fraudsters will often book round-trip tickets, with the intention of only using the outbound segment in order to avoid arousing suspicion. Chart #8 shows all the common indicators researched in the survey and how often they were noted as important in assessing risk.



8

Indicators of Fraudulent Bookings



BEST PRACTICE
advice

To better detect and prevent fraud, use multiple tools with proper fraud management practices and systems in place. A layered defense approach uses tools in each of the four dimensions of fraud detection. Think of each tool as a piece of a jigsaw puzzle – a single piece may show a part of the picture, but the more pieces you have, the more you can see the whole picture of fraud, and the more likely you'll be able to achieve better results.

Stage 2: Manual Review



Bookings which do not pass the automated screening stage typically enter a manual review queue. During this stage, additional information is collected to determine if bookings should be accepted or rejected due to excessive fraud risk. 85 percent of airlines surveyed indicated they manually review some bookings to manage fraud.

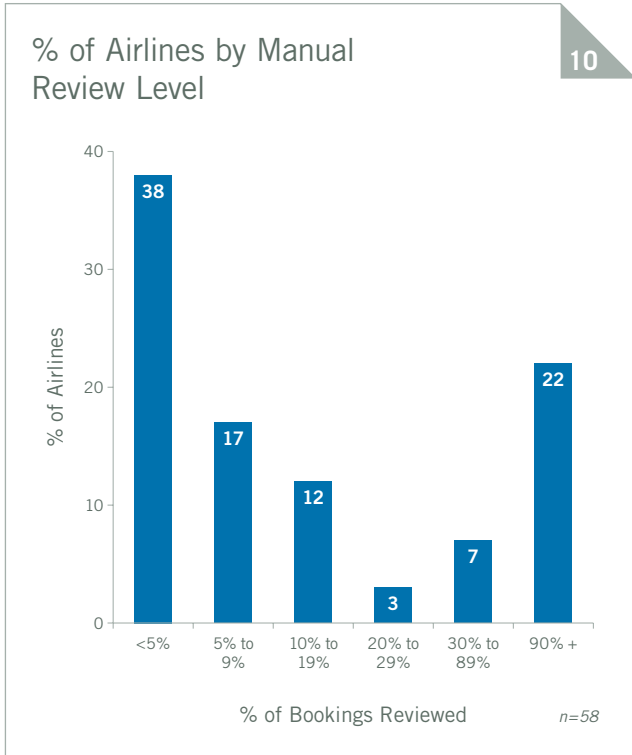
Manual review represents a critical area of profit leakage. It is expensive and difficult to scale in the face of seasonal peaks or growth, and may cause delays in ticket issuance, which can negatively impact the customer experience.

Manual Review Rates

In what should be a highly automated ticketing environment, most airlines are manually checking bookings. Today, on average, three out of ten bookings are manually assessed (which is nearly equal to non-airline industries, which average 33 percent⁶). However, as chart #9 shows, manual review rates vary widely.

Just over half of the airlines in the survey report reviewing less than ten percent of online bookings. However, one out of five airlines surveyed rely heavily on manual order review to catch fraud. 22 percent of airlines reported that they manually review 90 percent or more of online bookings for fraud, as chart #10 outlines. These airlines have a significant opportunity to reduce costs and increase automation.





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; 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

Reviewers disposition an average of 86 bookings each day. However, larger airlines in the survey reported an average of 98 bookings processed per reviewer per day, as shown in chart #11. This is very similar to the manual review productivity rates we see for large non-travel online merchants⁶.

Airlines with less than \$250 million in annual online revenues reported manual reviewer productivity that was half that of airlines with higher online sales volumes. Larger airlines use

more tools and often employ case management systems that allow reviewers to work more efficiently. Reviewers at large airlines spend an average of five minutes reviewing a booking, versus ten minutes for reviewers at smaller airlines. Looking at the total sample of airlines, the weighted average for online booking revenues per review staff was \$380 million per year per reviewer, with a median of \$120 million per year per reviewer.

Final Booking Disposition

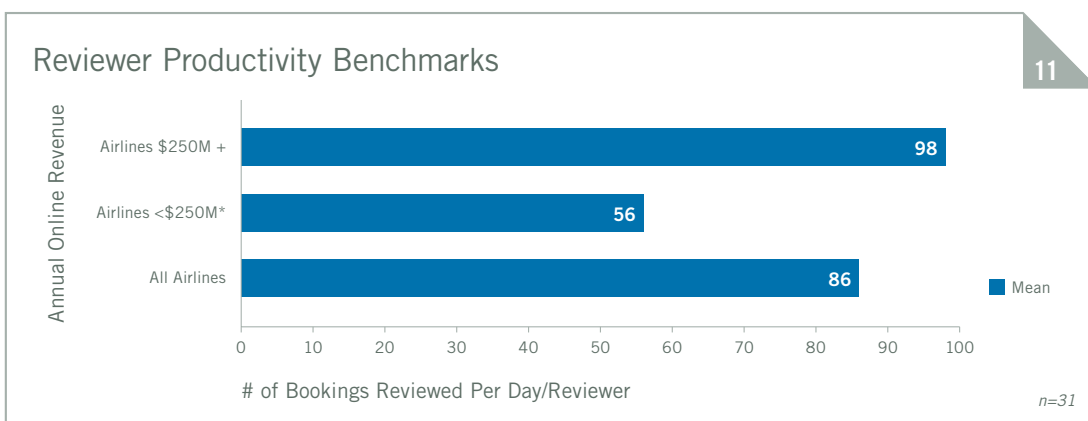
Automated screening and manual review ultimately result in booking acceptance or rejection. A relatively high percentage of bookings manually reviewed are ultimately accepted (see next section) – highlighting the need for airlines to improve automated screening accuracy and reduce the need for review. A look at order reject and acceptance rates follows in Stage 3 of the pipeline review.

BEST PRACTICE
advice

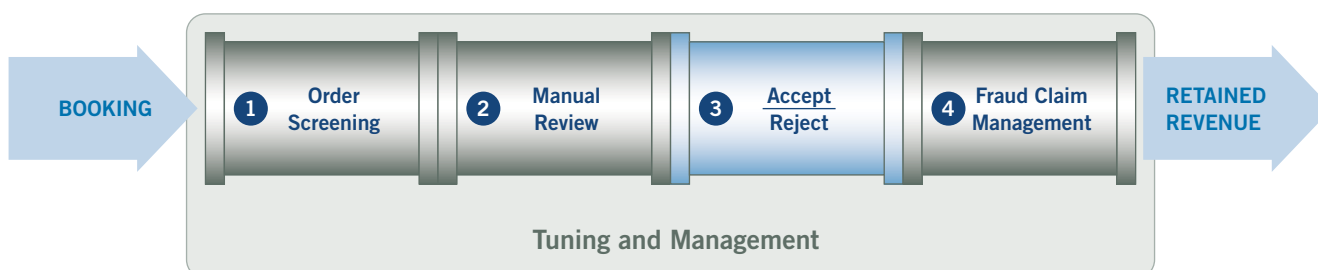
To help improve the efficiency and productivity of manual review staff, use an automated decisioning system with case management. Ensure that the system can be easily modified, and will allow you to customize or fine-tune rules to address particular fraud patterns. Without this ability, it's difficult to minimize reject rates, review costs, and fraud rates.

Reviewers have different levels of proficiency and approaches to assessing bookings, while staff turnover necessitates ongoing training. It can therefore be challenging to maintain a consistent level of fraud review quality without the aid of some automation.

A good case management system will provide a single portal through which pertinent data relating to the booking can be examined, and further investigative tools called on. This can help increase reviewer efficiency and reduce the time spent per review.

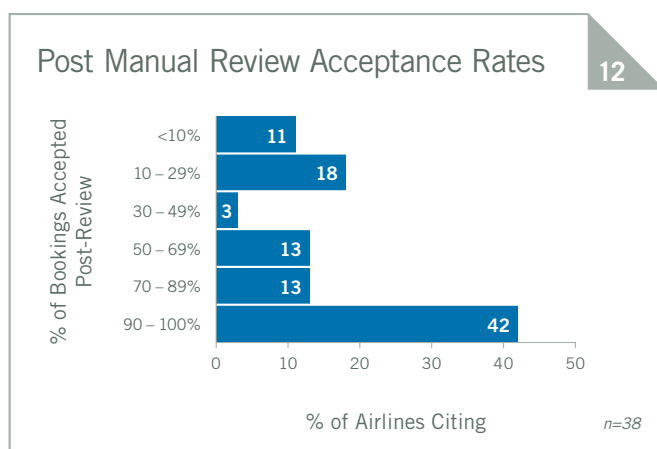


Stage 3: Order Dispositioning (Accept/Reject)



Post-Review Booking Acceptance Rates

Airlines that manually review bookings indicated they ultimately accepted 61 percent of such bookings (see chart #12). This compares to 73 percent for non-airline companies⁷. 42 percent of airlines surveyed report they accept 90 percent or more of the bookings they manually review. These carriers are incurring significant expense to find the ten percent or less of the review queue they believe to be too risky to accept.



Overall Booking Rejection Rates

Booking rejection rates can reflect true fraud risk, or signal “profit leaks” in terms of valid booking rejection or unnecessarily high rates of manual review. On average, airlines rejected 2.8 percent of their online bookings, but this varies widely by region – from 0.8 percent in North America to 8.4 percent in Africa (see chart #13). Non-travel merchants evidence similar overall average reject rates (2.9 percent in 2008⁸).

Airlines in North America typically use 7.5 fraud detection tools, which allow them to better screen for invalid bookings as compared to airlines in Africa, that use an average of 4.7 tools.

It is likely airlines will be under continued pressure to maximize every available revenue opportunity for the foreseeable future. Airlines should seek ways to accept more valid bookings and reduce those rejected due to suspicion of fraud without increasing headcount or other review costs.

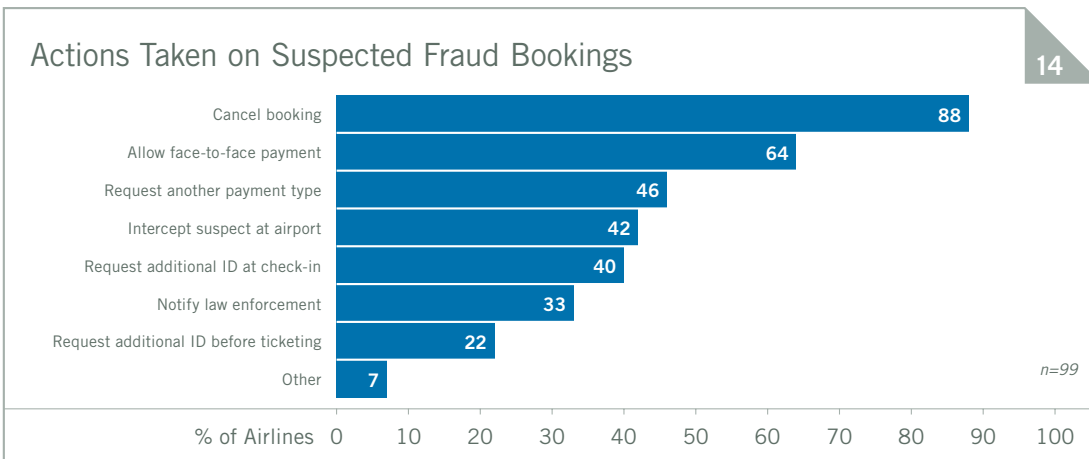
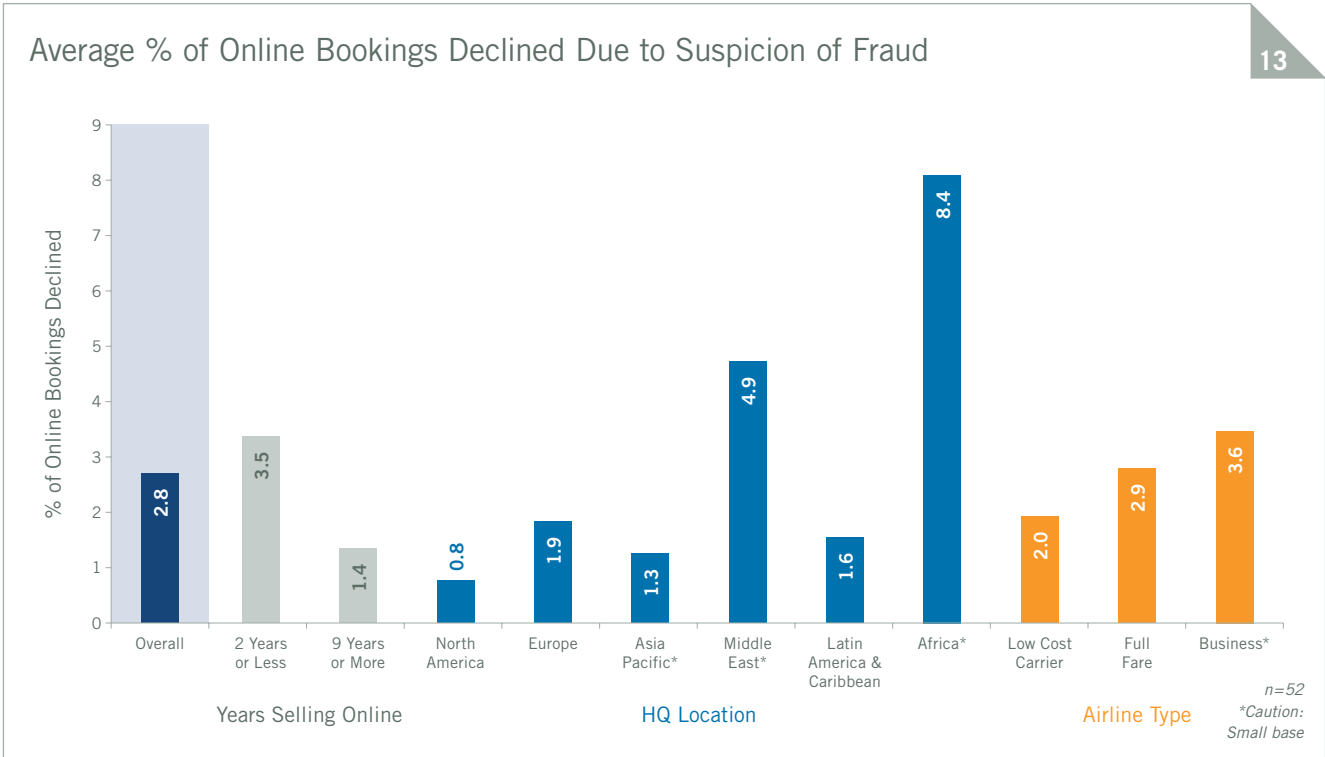
Actions Taken on Suspicious Bookings

Once a booking is suspected of being fraudulent, airlines employ various steps. As chart #14 highlights, the vast majority (88 percent) cancel some of the suspicious bookings. However, airlines may employ other actions, depending on their fraud management strategy.

Some carriers may be highly focused on revenue capture, so they will provide other payment options, by either requesting another form of payment during booking, or asking the purchaser to pay in person. For instance, 67 percent of North American airlines ask for another payment method, and 92 percent allow the purchaser to pay in person. In contrast, only 39 percent of European airlines solicit another payment method and only 50 percent of Asian airlines allow the purchaser to pay in person for suspicious online bookings.

Less frequently, airlines may also focus on validating the purchaser by requesting additional identification before ticketing or at check-in. More airlines request supplementary identification at check-in (40 percent) versus before ticketing (22 percent). This could be due to the high prevalence of electronic tickets, which by their very nature make requiring proof of identity a challenge.

However, asking for identification at check-in means that airlines may not have enough time to sell the seat and recover revenue if the traveler is denied boarding. It may also disrupt the boarding process and cause flight delays to require additional validation at check-in – something airlines are keen to avoid, given the need to check-in and board all passengers as quickly as possible.



BEST PRACTICE
advice

To improve the decisioning process, look to fine-tune your upfront fraud screening practices, so that only truly questionable bookings require a second look. Optimized upfront fraud screening can help reduce workload for your fraud review team, and minimize the need to add more headcount to manage fraud. With 61 percent of manually reviewed bookings ultimately accepted, it is clear most airlines require better methods to determine which bookings need to be outsourced for manual review.

You should also track fraud rates for online bookings that have been approved via manual review. 26 percent of the airlines surveyed do not track this metric. Without knowing this, systemic causes of fraud loss and process efficiencies between automated and manual review cannot be fully understood.

Lastly, to capture more revenue, consider offering other options for the purchaser to pay – only 46 percent of airlines surveyed requested another payment type as a means of substantiating a questionable booking.

Stage 4: Fraud Claim Management



Fighting Chargebacks

An apparent prevailing wisdom is that airlines should simply absorb fraud loss from chargebacks, which might explain why nearly one-third of the airlines surveyed fight less than ten percent of their chargebacks. Yet, as chart #15 shows, 34 percent of carriers surveyed contested over 90 percent of their chargebacks. This bi-modal distribution is consistent with non-travel merchants⁹ – a sizeable portion fight few chargebacks, and some fight them all as a matter of policy.

On average, airlines report that they win 47 percent of the chargebacks they dispute, recovering 32 percent of the chargebacks overall. **Methodology Note:** Because of the wide variance in chargeback representment practices, we calculated the net recovery rate for each airline participating in the survey and then averaged the result, which came to 32 percent.

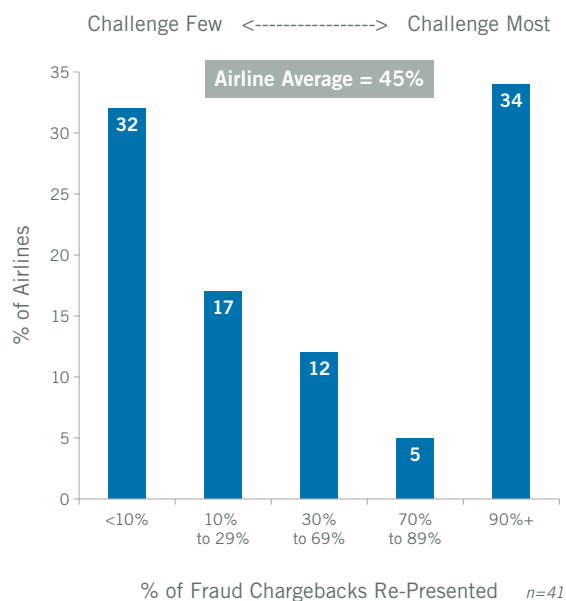
BEST PRACTICE advice

Consider disputing more of your chargebacks. Although it is not an easy or cost-free process, with an industry average 47 percent chargeback win rate, it may make good financial sense to re-consider your chargeback management policies and focus on recovering more revenue.

To successfully dispute chargebacks, make sure that you have easy access to a wide range of information about the chargeback, such as booking data and payment specifics. An efficient re-presentment process can help enhance profitability and reduce fraud loss.

Fraud Chargeback Re-Presentment Rates

15



Fraud Rate Metrics

When monitoring the level and trend of online fraud loss, we focus on two key metrics: 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). These fraud losses would include not only credit/debit card chargebacks, but also losses from other payment methods and any credits or refunds issued directly to consumers by airlines to avoid chargeback disputes and fees or to maintain customer goodwill.

As such, the survey loss rates tend to be higher than those reported by banks and credit card associations, which generally base reported rates on card chargeback activity only.

Fraud loss risk tolerances and booking rejection rates can vary significantly by airline. For instance, business class airlines have a higher reject rate, but lower overall fraud rate. Business class carriers, with higher priced seats, may err on the side of caution: rejecting more bookings to avoid expensive fraud losses. On the other hand, low cost carriers, with lower priced tickets, may allow more bookings to quickly fill seat capacity and maximize revenue. So, they tend to have lower reject rates but slightly higher overall fraud rates.

Direct Revenue Loss Rates

Airlines that have more years of online sales experience have a significantly lower fraud rate than those with less. The more experienced airlines typically use more tools and have additional resources to manage online fraud, so their fraud rates tend to be lower. Those with less than two years' online sales experience use fewer tools (4.6) and have a fraud loss rate that is over three times higher than airlines with nine or more years of online sales experience (3.8 percent vs. 1.1 percent, respectively). Chart #16 shows the distribution of loss rates reported by airlines responding to the survey.

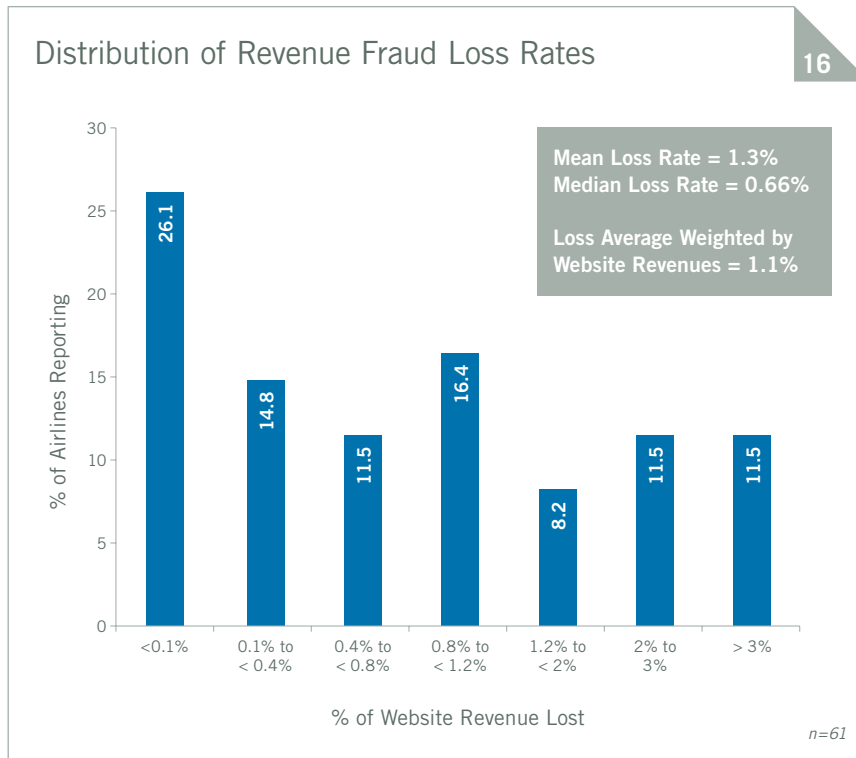
Fraud Rate for Accepted Bookings

The fraudulent booking rate is the number of accepted bookings that later turn out to be fraudulent, expressed as a percent of total bookings. Overall, airlines reported that, on average, 1.5 percent of their bookings resulted in payment fraud.

Figures for chart #17 include both chargebacks and credits issued directly by the airline in response to fraud claims.

BEST PRACTICE advice

Break out online revenues derived via your own website from total revenue. A significant number of airlines only track overall bookings, which makes it more challenging to capture true online payment fraud loss. Tracking online fraud loss by revenue and by booking, as well as your overall online revenue totals, will enable you to have a more complete picture of fraud occurring in the direct web channel.



Tuning & Management

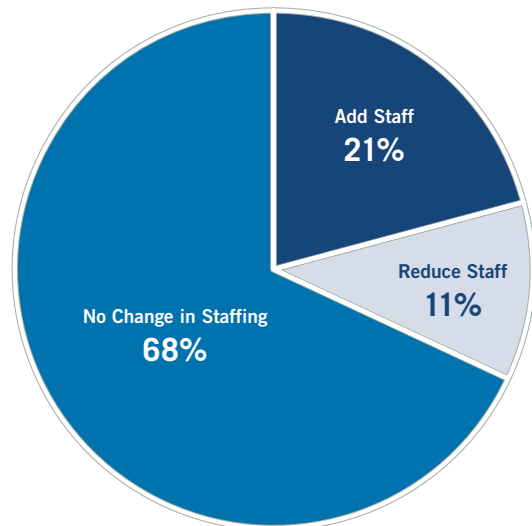


Fraud review staffing can be a sizable portion of fraud management budgets, as manual review can be labor-intensive and costly. 21 percent of airlines surveyed will be adding to their fraud review staff (see chart #18) in 2009. This may be viable short-term, but as the number of bookings fluctuates, scalability could become an issue. Even at a stable percent of bookings sent to review, the total number of bookings that must be reviewed grows in line with the total increase of online sales. Airlines simply cannot continue to add headcount to address fraud screening, without impacting the bottom line.

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.

Manual Review Staffing Levels – 2009 Plans

18



n=58

BEST PRACTICE advice

Look at integrating your fraud tools and strategies via fraud management portals. These portals employ a combination of flexible rules systems that interact with a portfolio of verification and validation services around the globe, allowing business managers in your company to set payment type, product type and market-specific screens.

Also, look for case management systems that are integrated into these portals with accompanying enhancements to streamline workflow.

Reducing the need for manual review and increasing reviewer productivity are key to maximizing profit while keeping your overall fraud management costs in line. One place to start is by improving the automated detection of risky bookings to reduce manual review volumes.

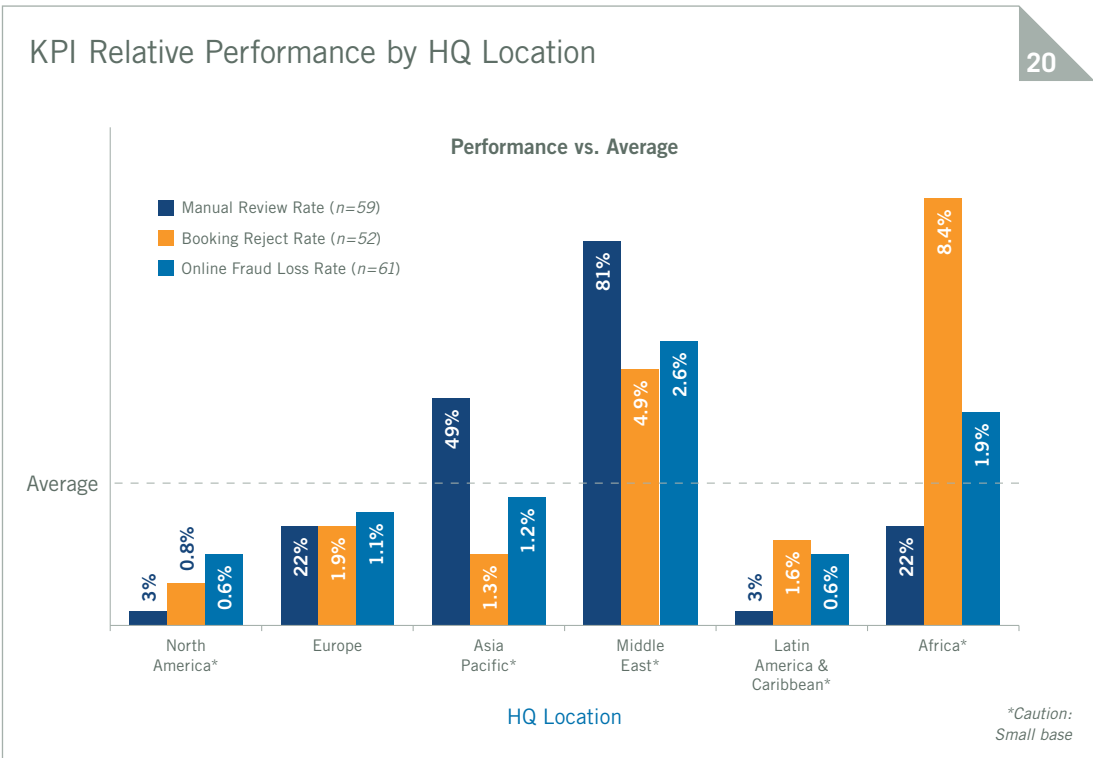
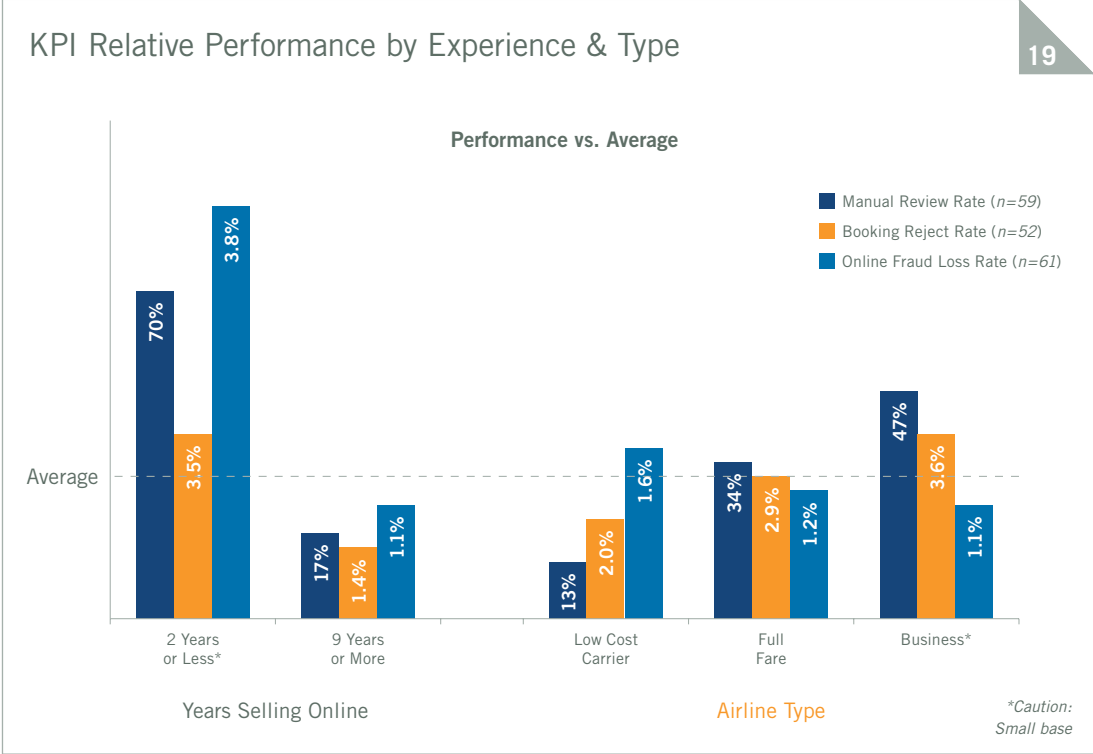
Conclusion

To arrive at 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 short, the survey results show that there is a wide range of practices and experiences among airlines with respect to fraud management and results.

Airlines with more years' experience selling online typically have more developed fraud management practices in place, resulting in lower fraud losses and lower manual review rates. Practices also vary by type of airline business model. Low cost carriers in the survey reviewed fewer bookings and used fewer tools while incurring above average fraud rates. In contrast, business class airlines reviewed a higher percentage of bookings, used more tools and rejected a higher percentage of bookings due to fraud risk, resulting in below average fraud losses (see chart #19).

KPIs also vary by region (see chart #20). Some of the differences are attributable to the type of airline as well as the years of online selling experience in those geographies, but some are due to the unique fraud challenges faced by airlines within those regions.

Ultimately the right fraud management process needs to be tailored for the unique situation, business goals and risk tolerances of an individual airline, to correctly optimize the trade-offs between review costs, booking rejection and fraud losses.



Resources & Solutions

To find information on CyberSource's industry-leading risk 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.

EMEA/APAC:

Visit www.cybersource.co.uk. For sales assistance, call +44 (0)118.929.4840 or email uk@cybersource.com.

CyberSource Risk Management Solutions

CyberSource's industry-leading risk management solutions enable airlines to retain more revenue and detect more online payment fraud. 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.

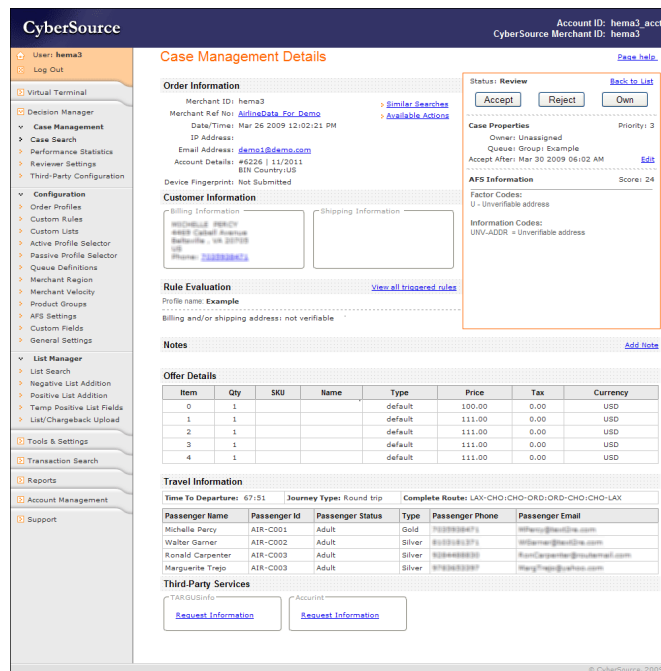
Decision Manager: Rule Console and Fraud Detectors

Decision Manager with CyberSource Intelligent Review Technology is a hosted system providing access to a full range of global fraud detectors, a business rule console that controls automated screening and case routing, and an advanced case management system.

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.

- On-demand access to 150+ global fraud tests across four dimensions of fraud detection
- Custom data imported from your systems to better screen for fraud, including names of travelers, routes, frequent flyer numbers
- A powerful business-user rule management console that enforces acceptance policies based on test results, to more accurately sort inbound bookings
- Automated case routing based on established rules, booking profiles, consolidated data review, and built-in callouts to validation services to streamline review, with automated queue management, including prioritization by flight departure times

- Supports any electronic payment channel, including call center and web
- Supports cards, direct debit, PayPal, Bill Me Later
- Works with any payment system or vendor



The screenshot shows the CyberSource Case Management interface. It includes a sidebar with navigation options like 'Virtual Terminal', 'Decision Manager', and 'Case Management'. The main content area displays 'Case Management Details' for a specific order. Key sections include:

- Order Information:** Merchant ID: hema3, Merchant Ref No: [Add/Update For Demo](#), Date/Time: Mar 26 2009 12:02:12 PM, Email Address: hema3@demo.com, Account Details: #6226 | 11/2011, BSN Country: US, Device Fingerprint: Not Submitted.
- Customer Information:** Billing Information (Name: Example, Address: 4567 Cabell Avenue, Berkeley, CA 94701, US, Phone: 5105551234) and Shipping Information.
- Rule Evaluation:** Profile name: Example, Billing and/or shipping address: not verifiable.
- Offer Details Table:**

Item	Qty	SKU	Name	Type	Price	Tax	Currency
0	1			default	100.00	0.00	USD
1	1			default	111.00	0.00	USD
2	1			default	111.00	0.00	USD
3	1			default	111.00	0.00	USD
4	1			default	111.00	0.00	USD
- Travel Information:** Time To Departure: 67:51, Journey Type: Round trip, Complete Route: LAX-CHO-ORD-ORD-CHO-CHO-LAX.
- Passenger List Table:**

Passenger Name	Passenger ID	Passenger Status	Type	Passenger Phone	Passenger Email
Michelle Tracy	AIR-C001	Adult	Gold	8008666666	WTracy@air.com
Walter Garner	AIR-C002	Adult	Silver	8008666666	WGarner@air.com
Ronald Carpenter	AIR-C003	Adult	Silver	8008666666	RCar Carpenter@air.com
Marguerite Trejo	AIR-C003	Adult	Silver	8008666666	MargTrejo@air.com
- Third-Party Services:** Includes links for 'Request Information' for TARUSInfo and Account.

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** to support 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 order review per your policies
- **Chargeback Recovery** where we examine, investigate and re-present your chargebacks

CyberSource Payment Management Solutions

In addition to our risk 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.

Accept All Popular Payment Types in 190+ Countries

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 percent of the tasks associated with payment reconciliation and chargeback re-presentation.

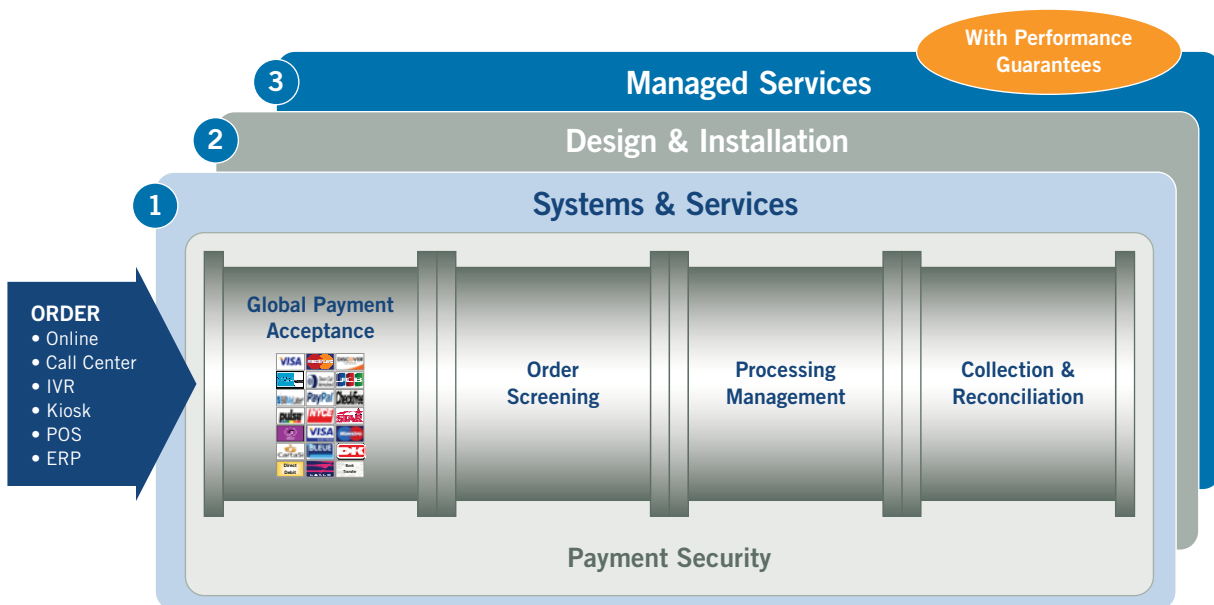
Payment Security

Remove payment data from your network. CyberSource provides secure storage and hosted payment acceptance services that let you process without storing or even transmitting payment data. A great way to streamline PCI compliance and mitigate security risk.

- **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.
- **PCI Planning & Remediation.** CyberSource provides PCI compliance consulting and remediation services to help remedy PCI issues.

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 Corporation is a leading provider of electronic payment, risk and security management solutions. CyberSource provides payment management solutions for electronic payments processed via Web, call center, kiosk, mobile and POS environments. Services include hosted systems to help you manage electronic payments, as well as professional services to help design, integrate and fully manage parts or all of your payment operations. Over 253,000 businesses worldwide use CyberSource solutions, including half the companies comprising the Dow Jones Industrial Average and leading Internet brands. The company is headquartered in Mountain View, California, and has sales and service offices in Japan, the United Kingdom, and other locations in the United States.

For More Information

Americas:

- Call **1.888.330.2300**
- Email **info@cybersource.com**
- Visit **www.cybersource.com**

EMEA/APAC:

- Call **+44 (0)118.929.4840**
- Email **uk@cybersource.com**
- Visit **www.cybersource.co.uk**

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 professional guidebooks in loyalty, CRM, eCommerce, payments, and ancillary revenue development. For more information please visit: <http://www.airlineinformation.org>.

North America

CyberSource Corporation
1295 Charleston Road
Mountain View, CA 94043
USA
T: 888.330.2300
T: 650.965.6000
F: 650.625.9145
Email: info@cybersource.com

Europe

CyberSource Ltd
The Waterfront
300 Thames Valley Park Drive
Thames Valley Park
Reading RG6 1PT
United Kingdom
T: +44 (0)118.929.4840
F: +44 (0)118.929.4841
Email: uk@cybersource.com

Japan

CyberSource KK
3-11-11 Shibuya, Shibuya-ku
Tokyo 150-0002
Japan
T:+81.(0)3.5774.7733
F:+81.(0)3.5774.7732
Email: mail@cybersource.co.jp