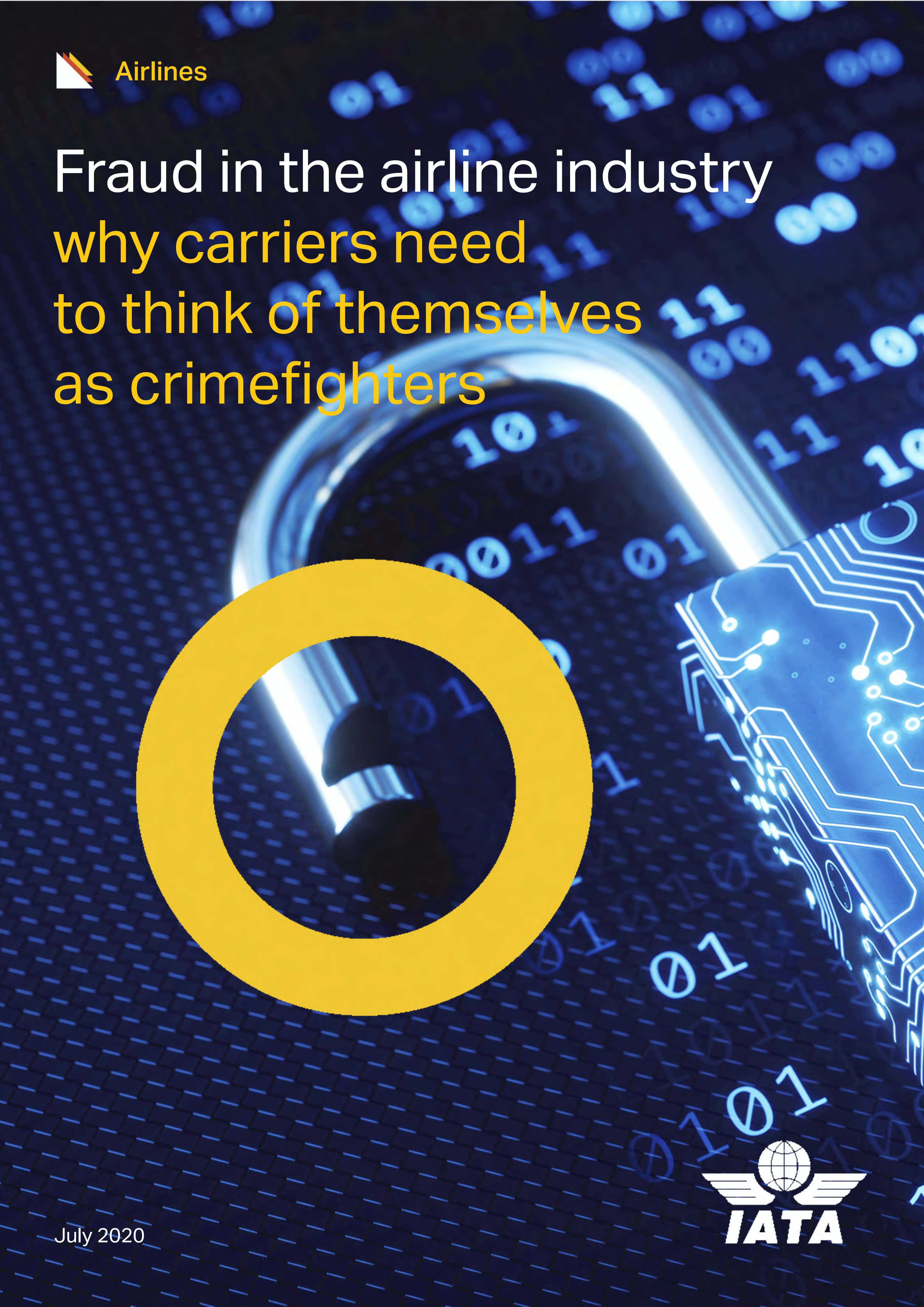
Airlines

Fraud in the airline industry why carriers need to think of themselves as crimefighters



July 2020

IATA

Fraud in the airline industry – why carriers need to think of themselves as crimefighters

What to expect from this white paper

Fraud affects airlines as much as any other industry. Commerce in air travel is often online – approximately 38% according to Amadeus and T2RL[1], and cross-border, making it a perfect target. It is also high value, with rewards being greater than the face value of what is defrauded. The ill-gotten gains of fraud committed against airlines enable further fraud and generate financial proceeds that are used to perpetrate illegal and reprehensible activities.

Payment fraud causes airlines to lose 1.2% of revenue annually of their website and mobile sales, according to Cybersource[2] (report conducted in collaboration with IATA and ARC). IATA latest estimates put this number at a minimum of $ 1 billion annually. And this does not include the impact on reputation, nor the cost of preventing and managing fraud, or even fraud in other other related areas such as frequent flyer programs.

A full understanding of how fraudsters operate is a first step in combatting fraud. This is however an ongoing process, as technology, attack methods, and industry responses evolve. It requires working together, as an industry, and as an anti-fraud community, sharing relevant information and best practices, and putting knowledge into action. In this whitepaper, IATA aims to give a good basic understanding of fraud in the airline industry, to indicate how to get involved in the community, and what airlines stand to gain from doing so. The contents are as follows:

Index

[1] "Global Airline Industry Almanac 2017 ↗

[2] "Benchmark Study: 2018 Global Airline Online Fraud Management", March 2018 ↗

Fraud is widespread, increasing and far-reaching

Fraud is organized crime

Fraud and cyber-crime will grow with further digital adoption

↓

Fraud is widespread, increasing and far-reaching

According to Nilson Report, from 2012 to 2018, fraud in online payments across all e-commerce types of business grew 240%[3]. Credit card payment fraud shows the greatest incidence. These sums have been steadily increasing with a 16% Compound Annual Growth Rate (CAGR), and a high proportion of this amount concerns Card-Not-Present (CNP) transactions.

Fraud levels are not equal around the world, however. Brazil, Mexico and Argentina experience the greatest fraud pressure – the highest number of attempts at fraud in a given period of time. It is mainly what is commonly known as "friendly" fraud – an illegitimate chargeback on a legitimate purchase, also known as cyber shoplifting. Next in line are China, the USA and France, where fraud attempts are more sophisticated and come in the form of account takeovers, bots and fake proxies.

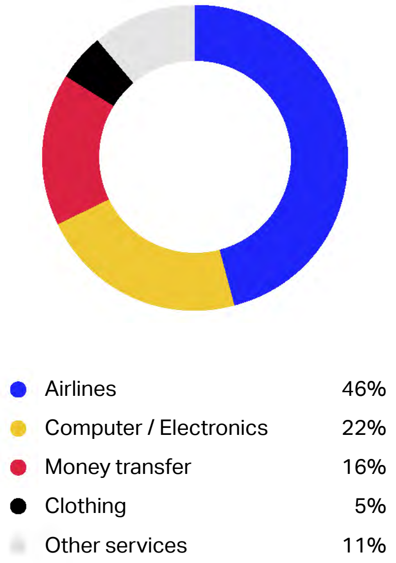
The inherent international scope of the airline business and its interdependency with technology, both for direct and indirect sales, mirror the mobility of fraudsters and their skillset. Additionally, its widespread acceptance of credit cards, and the relatively high value of its offer, contribute to exposing it to high levels of fraud. **According to RSA Security and Juniper**[4]**, airlines are in fact the vertical most affected by online fraud, accounting for 46% of fraudulent transactions**. Money transfer and computers/electronics Money transfer and computers/electronics are much less impacted at respectively 16% and 13%. **From 2018 to 2019 alone, fraud attacks on the airline sector increased by 61%, as per latest Forter Fraud Report**[5]. Additionally, **the average value of a fraudulent air ticket purchase is significantly higher than that of the average value of a legitimate purchase**, with fraudsters targeting upper-tier products. The average legitimate purchase is worth US$606, while the average fraudulent purchase is more than three times higher, at US$1,930[6].

[3] Card Fraud Worldwide 2010-2027,Nilson Report, November 2019 ↗

[4, 6] Juniper Report "ONLINE PAYMENT FRAUD WHITEPAPER 2016-2020" ↗

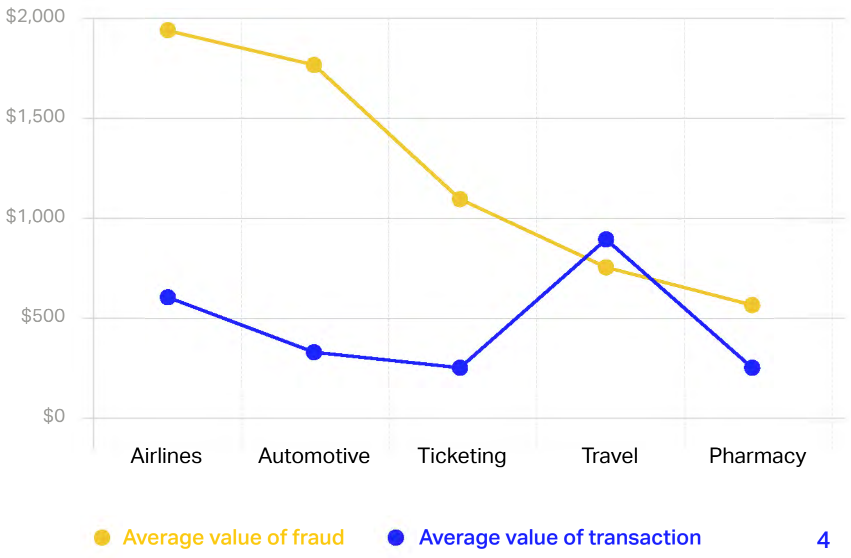
[5] Forter – Fraud Attack Index, 7th edition – 2019 ↗

Top Merchants Affected by Fraud Transactions



Average Value of Fraud Transactions

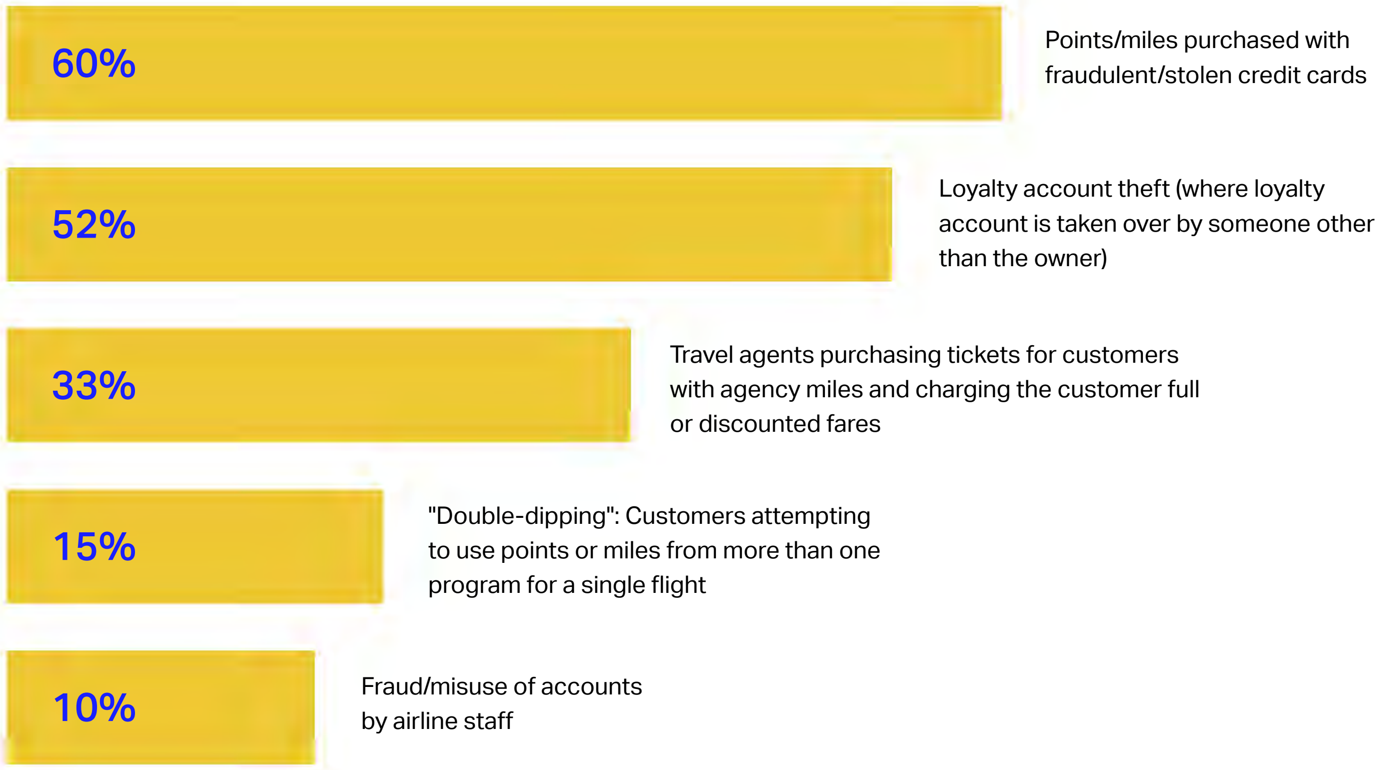
Source:
[4] RSA Security



Fraud is widespread, increasing and far-reaching

And it is not just air ticket purchases that are being defrauded. Fraudsters have also exploited airline Frequent Flyer Programs (FFP). Unfortunately, sometimes FFP fraud is only discovered by pure accident. A large volume of unredeemed miles could become a serious liability for the airline financials. In addition, loyalty programs generate revenue, as well as being important sources of customer data. It is therefore in the interests of airlines to protect this investment in customer relations.

Common Types of Loyalty Program Fraud



Source:
[2] Cybersource
"Benchmark Study: 2018 Global Airline Online Fraud Management"

Fraud is widespread, increasing and far-reaching

Fraud is organized crime

Today, defrauding an airline is not just about getting a free business-class trip to a far-off destination. According to Dr. Michael McGuire, criminologist, cybercrime across different industries generates a minimum of $1.5 trillion in revenue every year for all those involved[7].

There are multiple types of fraud techniques that can take place along a process, that start in the theft of information to end up committing a fraudulent payment. Here are some of the most common ways they obtain those tickets or funds:

> "According to Dr. Michael McGuire, criminologist, cybercrime across different industries generates a minimum of $1.5 trillion in revenue every year for all those involved."

Online ticket fraud, also called Card-Not-Present (CNP) fraud

With deep knowledge of the way the travel industry functions, fraudsters book near-term departures, for any ticket value, with airlines and Online Travel Agent (OTA) websites, during 'out-of-office' hours, when trained staff have handed over to less-experienced call center personnel. They pay using stolen credit cards or other Forms of Payment (FOP) such as debit cards or e-wallets.

Loyalty fraud

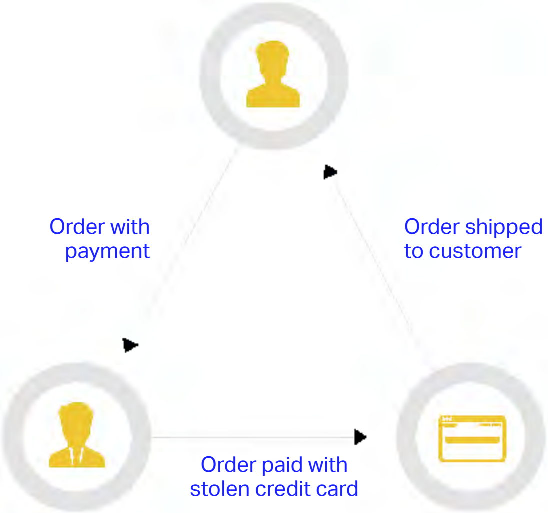
To access FFP member accounts, fraudsters use password hacking and phishing and even resort to compromising employees. Once access is gained, they purchase tickets for resale or for use by criminals, or redeem stolen miles against partner offers, such as hotel accommodation, car rental, stores, etc.

[7] Into the Web of Profit: Tracking the Proceeds of Cybercrime RSA Conference 2018 ↗

Fraud is widespread, increasing and far-reaching

Fake travel agent sites, also known as triangulation scheme

Bookings on fake travel-agency websites notify a fraudster who books an actual flight with fake payment information, and re-sells it to the trusting customer for the advertised incredible discount. There are potentially three victims in these cases: the passenger, who will not be able to fly, the airline, which is out of pocket the actual cost of the ticket, and perhaps an intermediary travel agent.



- Unsuspecting customer places an order on an auction or fake marketplace using some form of payment
- Fraudulent seller receives the order and then places the same order for the actual product with a legitimate eCommerce website using a stolen credit card
- Legitimate eCommerce website processes the fraudster's order

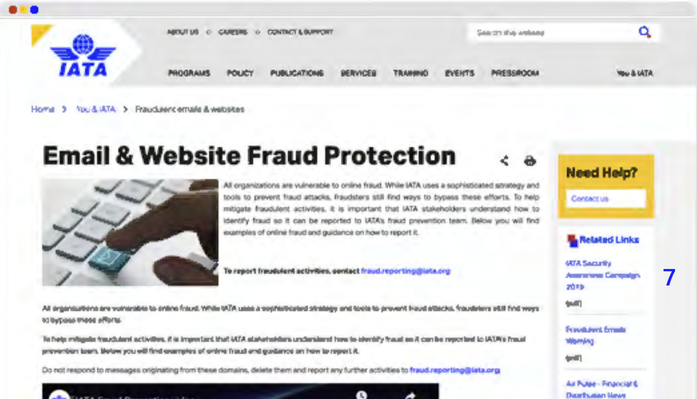
In-flight fraud

Using counterfeit credit cards, fraudsters purchase duty-free products, aware that onboard payment terminals are offline, and no authorization request can be carried out. The goods are then re-sold at a markup.

Baggage fraud

Checked-in carry-ons are declared lost at destination, and claims are for high-worth contents. Fake receipts back up insurance claims.

Beware of the latest phishing attacks by fraudsters using IATA's identity. You can consult latest information and report suspected scams on ↓


ABOUT US
CAREERS
CONTACT & SUPPORT
Search the website
IATA
PROGRAMS
POLICY
PUBLICATIONS
SERVICES
TRAINING
EVENTS
PRESSROOM
You & IATA
Home > You & IATA > Fraudulent emails & websites
Need Help?
Contact us
Related Links
IATA Security Awareness Campaign 2019 (pdf)
Fraudulent Emails Warning (pdf)
Air Pulse - Financial & Distribution News

Email & Website Fraud Protection

All organizations are vulnerable to online fraud. While IATA uses a sophisticated strategy and tools to prevent fraud attacks, fraudsters still find ways to bypass these efforts. To help mitigate fraudulent activities, it is important that IATA stakeholders understand how to identify fraud so it can be reported to IATA's fraud prevention team. Below you will find examples of online fraud and guidance on how to report it.

To report fraudulent activities, contact fraud.reporting@iata.org

All organizations are vulnerable to online fraud. While IATA uses a sophisticated strategy and tools to prevent fraud attacks, fraudsters still find ways to bypass these efforts.

To help mitigate fraudulent activities, it is important that IATA stakeholders understand how to identify fraud so it can be reported to IATA's fraud prevention team. Below you will find examples of online fraud and guidance on how to report it.

Do not respond to messages originating from these domains, delete them and report any further activities to fraud.reporting@iata.org

→ index

Fraud is widespread, increasing and far-reaching

Fraud and cyber-crime will grow with further digital adoption

There are many reasons why fraud is increasing. One is the change in consumer behavior. Since the advent of e-commerce, consumers have embraced online shopping. They browse and compare, and geographical borders mean little to them, unless restricted. As time has gone on, the flow of money online has increased, providing more opportunities for fraudsters. As technology has evolved, mobile payments have increased, particularly in emerging markets. Merchants report more attempts at fraud through the mobile channel, largely through mobile wallets.

As well as increasing, **fraud is becoming more sophisticated**, with perpetrators using new technologies and attack methods. **Only in the second half of 2018, 2.1 million bot attacks on e-commerce sites were reported**[8]. Cybercrime is also becoming more professionalized, as can be seen with the number of cybercrime experts and the technical availability of cybercrime tools such as malware.

Firms, however, have not been keeping up with this sophistication, **and it is increasingly difficult for businesses to keep up with the size of the problem**. Breaches affect the rate of fraud in more ways than one. Insufficient security can lead to direct fraud on a platform, or it can provide fraudsters with sensitive and complete information about customers that can be used to commit fraud in different ways later, such as creating credit accounts. The 2017 Verizon Data Breach Report cites that 81% of hacking-related breaches in USA leveraged either stolen and/or weak passwords, up from 63% reported in previous years[9].

Rigorous authentication is the first defense in cybersecurity, but companies are struggling to reconcile their aim of frictionless user experience with an increased number of steps in the login process. Weak security goes beyond passwords, of course, and the data breaches suffered by several major companies around the world in recent years highlight other deficiencies in company systems, both technology- and people-related. This is a trend that is not set to diminish. Advances in technology are disrupting many industries and creating new ones, and these transformations could increase companies' exposure to cybercrime if not addressed in depth.

> Rigorous authentication is the first defense in cybersecurity, but companies are struggling to reconcile their aim of frictionless user experience with an increased number of steps in the login process.

[8] Forbes ↗

[9] 2017 Verizon Data Breach Report ↗

2

Fraud has an impact on airlines' profitability

Damage is not always obvious

How good are airlines at fighting this crime?

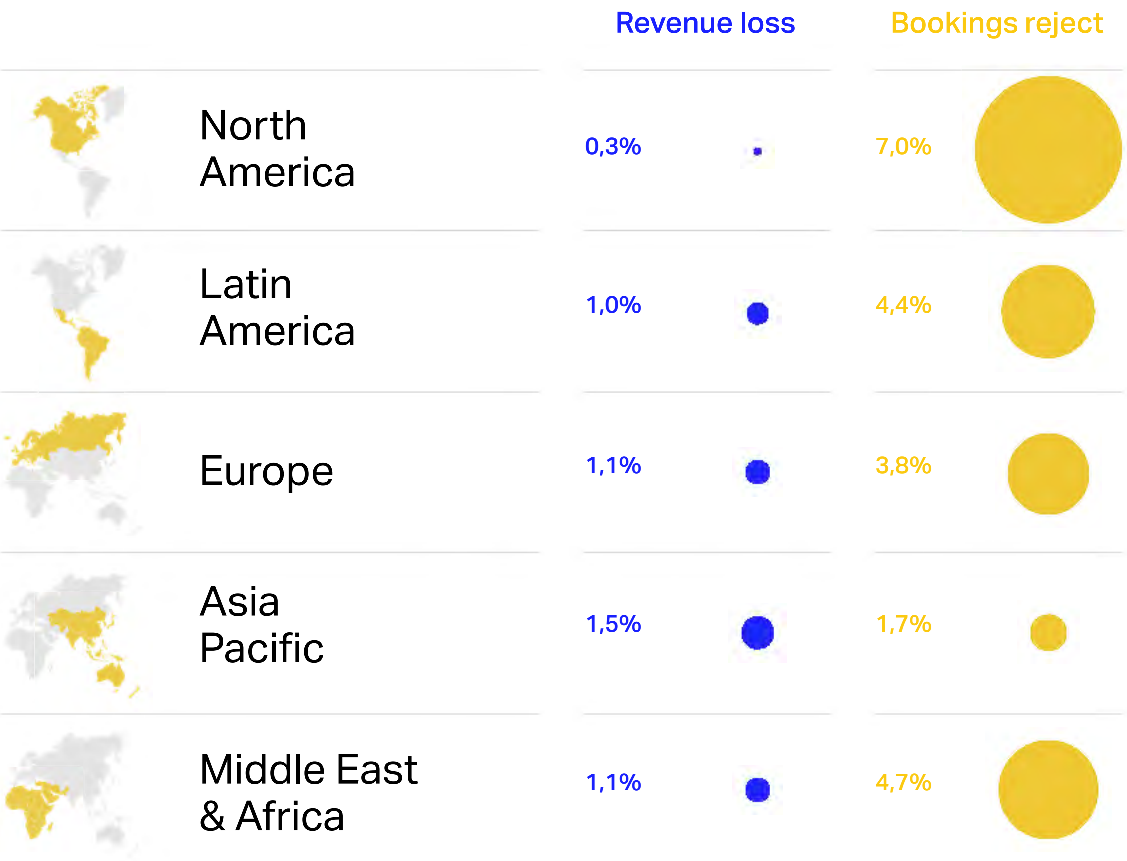
↓

Fraud has an impact on airlines' profitability

The expression 'fraud loss' can be defined as the incurred loss, cost or expense which is not reimbursed and arises out of the fraud committed. It is the value that has been written off as unrecoverable as a result of theft or compromise. Unlike "necessary" costs, such as staffing, utilities, procurement, accommodation etc., fraud loss is considered "unnecessary".

Thinking about it only as a cost of doing business, however, minimizes its actual impact. In fact, fraud has a direct economic impact in the topline of online businesses. Sales are a business's life force. Every legitimate sale is like a breath of clean air to a company. Every fraudulent transaction is a polluted one. There is an inverse relationship between bookings rejected and revenue loss: the more bookings the airline reject, the less revenue it loses.

Some countries, it appears, are better at filtering the air they breathe. This could be explained by the fact that the countries of North America and Europe have had to contend with more fraud historically and have been more aggressive in fighting it. Should fraud attempts become more vigorous in other regions, it is likely that efforts to stop them will increase, which will reduce revenue loss in these areas.



	Revenue loss	Bookings reject
North America	0,3%	7,0%
Latin America	1,0%	4,4%
Europe	1,1%	3,8%
Asia Pacific	1,5%	1,7%
Middle East & Africa	1,1%	4,7%

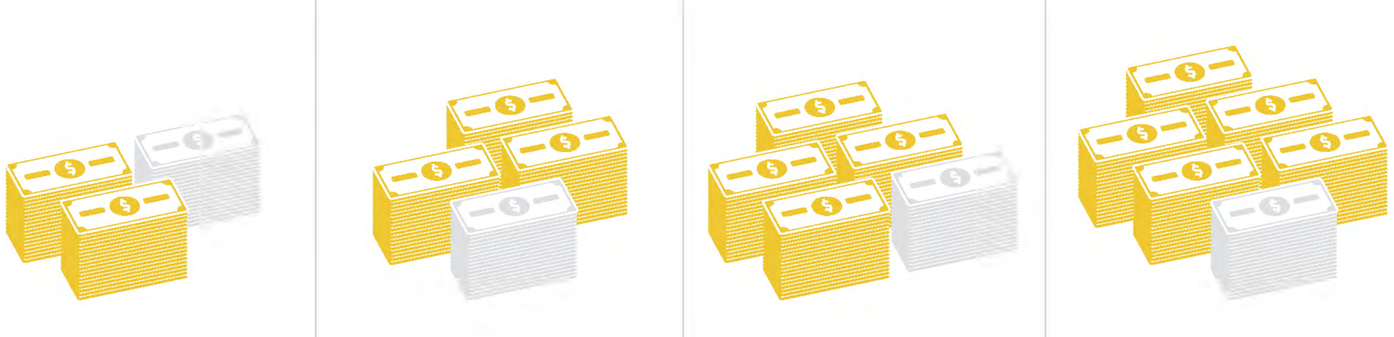
Source:
Cybersource report

Fraud has an impact on airlines' profitability

Damage is not always obvious

What impacts the top line, naturally has a knock-on effect on the bottom line. The importance of this effect will depend on the gross margin: the lower the margin, the greater the impact of fraud will be. This is called **the multiplier effect of fraud**. Going back to previous analogy, the more trouble one has breathing, the worse pollution will affect you.

Payment fraud loss of revenues may impact the operating margin of the airline significantly

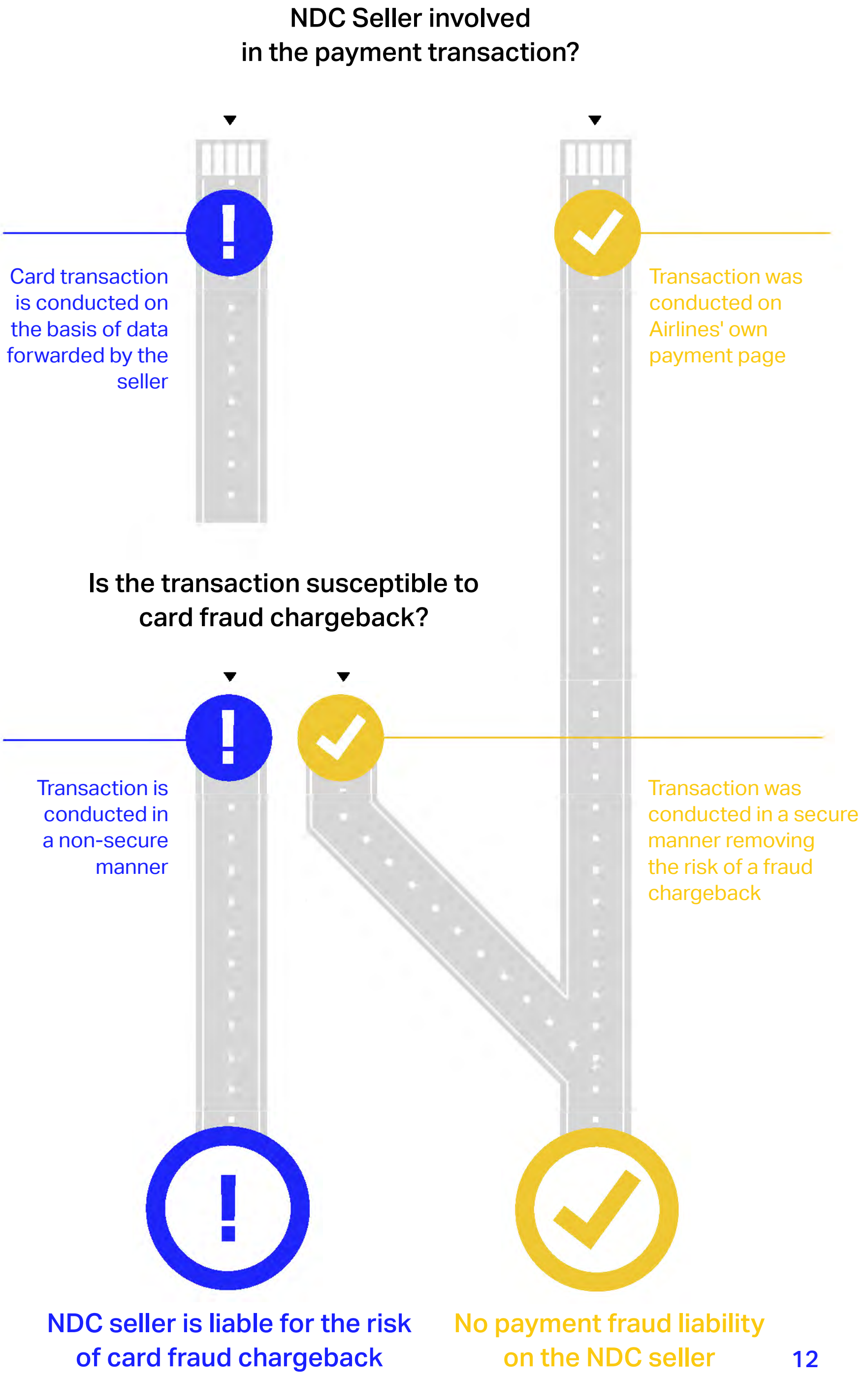


Fraud has an impact on airlines' profitability

However, it is important to note that the impact on airlines and travel agencies can be very different. In the direct channel, in the case of a stolen credit card being used for a transaction for example, in most instances the airline will have to absorb the cost of a chargeback following the claim made by the legitimate cardholder and the bottom line impact will depend on the airline's margin. In the indirect channel, IATA member airlines can pass the loss on to the travel agency, via an Agency Debit Memo (ADM), in accordance with Passenger Conference Agency Resolution Resolution 890. The travel agency is therefore liable for the total amount of the fraudulently purchased ticket. The direct cost to the airline, however, is limited to the operational cost of carrying the fraudster, a fraction of total revenue from the flight, as any other transaction.

New Distribution Capability (NDC) standard adoption will generate a major change in the way fraud is managed in the indirect channel. Relevant industry governances are working on Resolution 890 to make it fit the NDC standard[10]. The risk of credit card payment fraud will remain the same as in the Global Distribution System (GDS) environment, but as contemplated under NDC it will have to be managed by airlines, which will require close collaboration between airlines' fraud prevention and distribution teams.

Principles for an NDC payment fraud liability shift



NDC Seller involved in the payment transaction?

Card transaction is conducted on the basis of data forwarded by the seller

Transaction was conducted on Airlines' own payment page

Is the transaction susceptible to card fraud chargeback?

Transaction is conducted in a non-secure manner

Transaction was conducted in a secure manner removing the risk of a fraud chargeback

NDC seller is liable for the risk of card fraud chargeback

No payment fraud liability on the NDC seller

Note:
Whether a transaction is susceptible to fraud liability or not also depends on the rules of the card scheme

Examples:
a 3DS transaction is not susceptible to fraud chargeback

a Visa transaction was approved by issuer despite CVV2 mismatch, the transaction is not susceptible to card fraud chargeback

[10] IATA Resolution 890

Fraud has an impact on airlines' profitability

But airlines should not be tempted to brush this off as inconsequential. Again, the industry could take into account the indirect cost of fraud when considering the impact on airlines' bottom line. This includes internal fraud management teams, but also IT security professionals, fraud investigators, externally managed fraud detection software services and legal advice.

The industry should take also into account the cost of damage to the brand and the associated loss of custom, particularly when it is not put right satisfactorily. According to management consultants Oliver Wyman, both externally and internally perpetrated *"Fraud cases lead to significant reputational impacts on the impacted institution, with the additional reputational loss predicted to be ~140% of the announced loss.*[11]*"*

> *"Fraud cases lead to significant reputational impacts on the impacted institution, with the additional reputational loss predicted to be ~140% of the announced loss."*

[11] The Hidden Cost of Reputation Risk – Oliver Wyman 2017 ↗

Fraud has an impact on airlines’ profitability

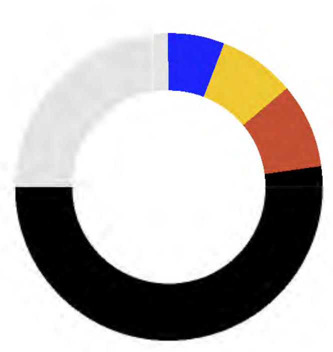
How good are airlines at fighting this crime?

In the airline industry, payment fraud is measured in the gross amount of fraud chargeback and rejected bookings. In most of the world, **the average rate of bookings rejected is 3.8%**, though North America experiences double that[12]. This could mean that North American airlines are more cautious and that they are potentially sacrificing valid orders. Overall, **full-service carriers reject over twice as many bookings as low-cost carriers, at 4.5% compared to 2%**[13]. Fraud pressure can reach a significant percentage of online transactions received, but it can also be reduced with competent anti-fraud measures; after being thwarted for a while, fraudsters will move on to easier pickings.

Globally, in all sectors of e-commerce where credit cards are concerned, the fraud-coded chargeback rate is estimated at 0.47%[14]. Japan rates are the lowest at 0.3%, bringing down the average. In Mexico, however, observed rates reach 1.3%. Local factors and banking practices that make chargebacks easier explain these high rates compared to the rest of the world.

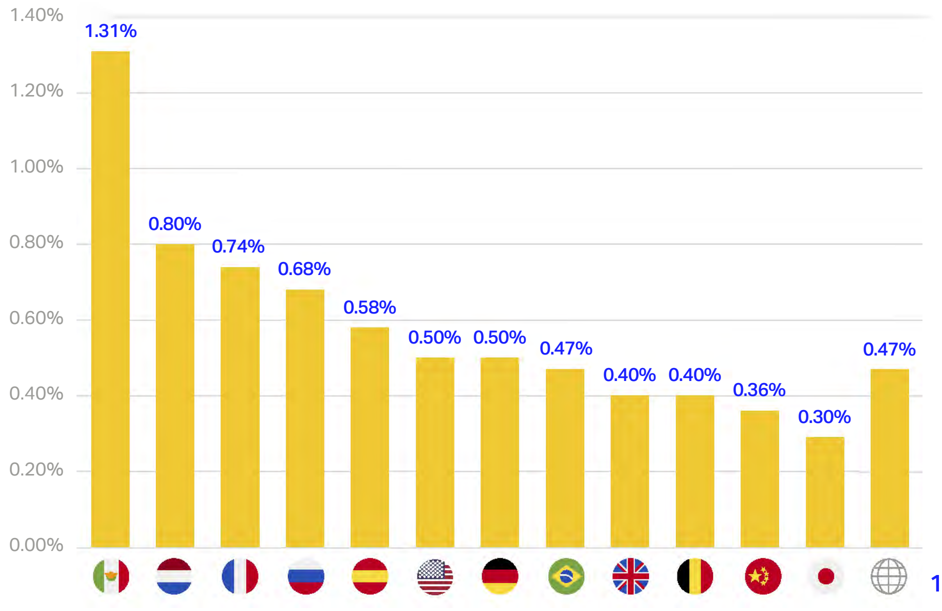
> “In the airline industry, the average rate of bookings rejected is 3.8%”

Top Countries by Attack Volume*



●	Netherlands	6%
●	China	8%
●	UK	9%
●	US	52%
●	Others	25%

Percentage of transaction Value Reported as Fraud Chargeback by Country (any e-commerce sector)**



* Source:
[14] RSA Security

** Source:
[14] Ingenico Payment Services

[12, 13] “Benchmark Study: 2018 Global Airline Online Fraud Management”, March 2018 ↗

[14] Juniper Report “ONLINE PAYMENT FRAUD WHITEPAPER 2016-2020” ↗

Forewarned is forearmed – what airlines need

Tools and best practices are the industry weapons

Innovation can help airlines win the battle

↓

Forewarned is forearmed – what airlines need

To understand how to better combat fraud, airlines first need to be aware of how fraud is carried out. “Payment fraud”, an illegal transaction that is unauthorized, or diverts merchandise, or where funds are unavailable (including false requests for refunds or returns), is but the tip of the iceberg. It is most commonly carried out using stolen or lost credit cards or card information. Although widespread, it occurs as isolated cases, with fraudsters using the credentials as soon as they obtain them. Payment fraud losses from e-commerce, airline ticketing, money transfer, and banking services, are predicted to grow, but this type of fraud is losing favor with fraudsters, who are starting to prefer more elaborate methods, which are harder to identify and provide higher rewards.

These more elaborate methods start with theft of information, including data breaches, malware and phishing. Employee account phishing is an example. Fake emails enable fraudsters to obtain employee credentials. Since employees often have access to customer credentials and, in the travel industry particularly, this information can be quite full, that’s a lot of information cybercriminals can re-use.

Stolen information is then tested and used in different ways. Fraudsters might mix it with fake information to create new identities – so called “synthetic users” – that can then be used to make fraudulent transactions. Large amounts of personally identifiable information (user names and passwords, for example), the product of massive data breaches, are now widely available for purchase. This can be used to set up automated logins to try and gain access to private accounts on a massive scale and take them over.

Such Account Take Over (ATO) concerns bank accounts, online or e-commerce accounts, and loyalty accounts. Fraudsters take advantage of the financial information already linked to the account, and add new information obtained through illicit methods. Fraud committed through a bona fide account that has been taken over is hard to detect. Only if there is a sudden and notable change to the account or in the buying pattern of the legitimate customer might a flag be raised.

Fraud types summary

Information theft	Information testing	Account theft/creation	Fraudulent payment	Physical goods delivery
Data breach	Credential stuffing		Payment fraud	Re-shipping
Malware	Card testing	Synthetic user	Loyalty fraud	
			First party fraud	
Phishing		Account takeover ▶	Account takeover	
Employee account phishing	⟶	Employee account takeover ▶	Employee account takeover	
			Merchant	

Source:
IATA internal analysis

Forewarned is forearmed – what airlines need

As mentioned, ATO also affects loyalty schemes. As indicated earlier, according to Cybersource's 2018 Global Airline Online Fraud Management survey, "loyalty account theft" is the second most common type of loyalty fraud in the airline industry (cited by 52%). "Points/miles purchased with fraudulent/stolen credit cards" has the top spot (cited by 60% percent of airlines). Fraudsters later redeem the funds that loyalty points represent, either buying tickets, purchasing merchandise, or cashing them in, and loyalty fraud is on the rise.

Tools and best practices are the industry weapons

Of course, while knowledge of how fraud is committed is key, it is not enough to prevent it. **Following best practices in fraud detection and prevention is a first step**. Where credit cards are concerned, real time authorization requests is an absolute requirement, as is obtaining Card Verification Numbers (CVN) - used by 78% of airlines - which cannot be calculated by fraudsters. In countries that support it, (USA, UK and Canada), verifying the address of the cardholder via the Address Verification Service (AVS) field is an additional safeguard - used by 50% of airlines[15].

Some 86% of airlines also either use or are planning to implement **3D Secure[16], a card industry standard protocol to have the issuer authenticate and approve their cardholder, which protects the merchant from fraud chargeback by a liability shift.** Please, note that 3D Secure is mandatory in Europe under Payment Services Directive 2 (PSD2).

These validation tools are the first front in the fight against fraud, and they are backed up by data tools and purchase-device tracking. On average, merchants use between 10 to 15 different variables to prevent fraudulent transactions, and this number has increased in recent years as new technologies have given us access to greater amounts of information.

Exchanging best practices through fraud forums and events, and consulting publications by industry bodies is also essential for airlines to ensure they stay updated with the latest developments. The Merchant Risk Council ↗ is a good example, and fraud conferences are occasionally organized by card schemes or other private organizers.

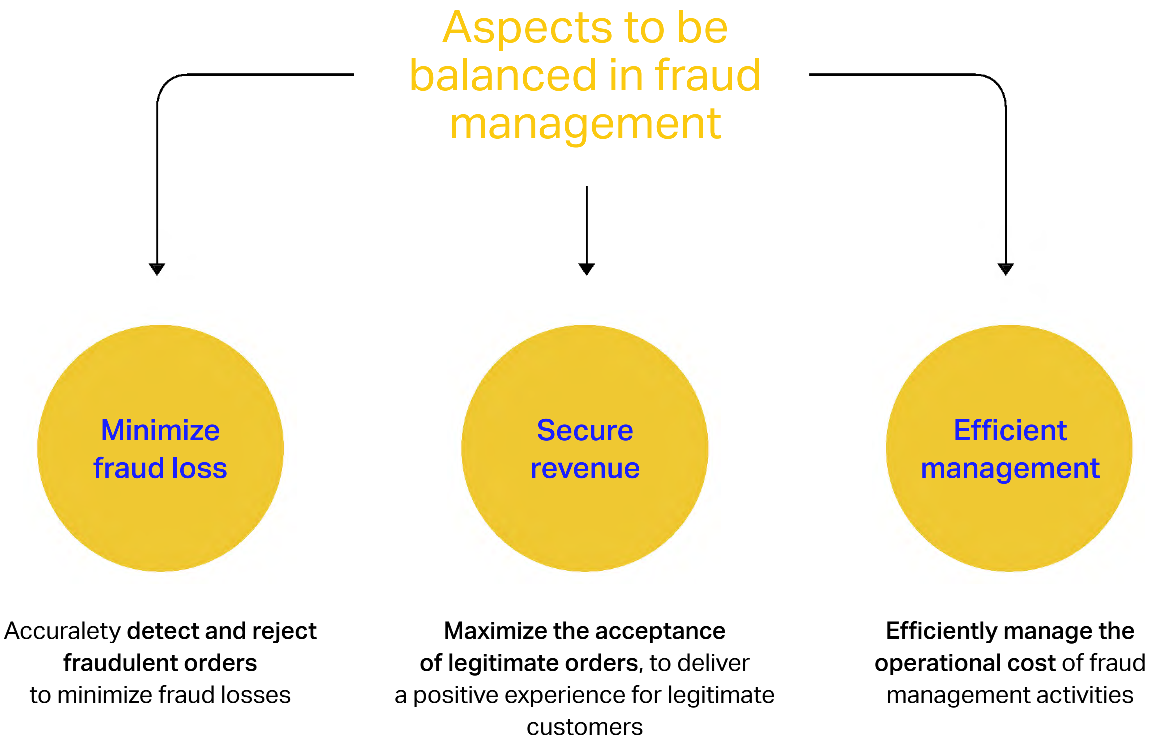
[14, 15] "Benchmark Study: 2018 Global Airline Online Fraud Management", March 2018 ↗

Forewarned is forearmed – what airlines need

However, properly managing fraud according to best practices has proven challenging for airlines. Some may not have enough internal resources or expertise. Lack of resources is understandable when significant percentages of airline direct bookings require manual review. Others do not have the technologies they need, including the ability to track various Key Performance Indicators (KPIs). Some are struggling to keep compliant as regulations change and improve, adding reporting obligations and fixing different thresholds according to country or region. Automation and systematization are therefore high on the list of airline priorities to help improve performance.

Innovation can help airlines win the battle

Fraud continues to evolve quickly, requiring an innovative approach to manage it, and the implementation of more sophisticated solutions. **Optimal fraud management is a balance of three key aspects: accurately detecting and rejecting fraudulent orders to minimize fraud losses; efficiently managing the operational costs of anti-fraud activities; and maximizing the acceptance of legitimate orders, to deliver a positive experience for legitimate customers.** This is no easy objective to attain, but trends are moving solutions closer.



Aspects to be balanced in fraud management

Minimize fraud loss

Accuralety **detect and reject fraudulent orders** to minimize fraud losses

Secure revenue

Maximize the acceptance of legitimate orders, to deliver a positive experience for legitimate customers

Efficient management

Efficiently manage the operational cost of fraud management activities

Source:
IATA internal analysis

Forewarned is forearmed – what airlines need

Airlines are strengthening their fraud-fighting capabilities, enabling better detection and rejection. They are adopting holistic management of fraud throughout the entire company, rather than channel by channel. In this way, they can consolidate their fraud management teams. This approach also allows them to redesign the customer journey, where necessary, with the aim of reducing the impact of fraud management techniques, such as authentication, on the customer experience. **Leading companies are adding weapons such as visual monitoring, alerts, robotics, lean management and interactive dashboards to their arsenal, helping them to speed up their fraud decision-making**. Other companies, those which have grown quickly and not been able to build in-house capabilities, for example, are augmenting their forces with the superpowers of fraud specialists. And this can benefit the whole industry. Fraud reduction is a shared objective within an economic sector, and specialists who work with multiple companies are able to pass along the benefits of their experience.

Advanced analytics techniques are like microscope or magnifying glass, improving the effectiveness and efficiency of fraud management, thereby reducing costs. **The integration of high-quality data sources and the use of new modeling techniques are transforming fraud prevention. Machine Learning (ML) is the first technique being used, to speed up decision-making, improve accuracy and reduce costs**. With the rise in ML, this branch of artificial intelligence has become a key technique for solving problems in very diverse areas, and is recommended for complex tasks or problems involving large amounts of data and lots of variables, but no existing formula or equation. This is the case in fraud detection, where the rules of a task are constantly changing with each introduction of new tactics by fraudsters. **ML models continually analyze and process incoming data, and autonomously update with the new information, making ML an effective tool for detecting the most common types of fraud such as payment fraud, account takeovers (whether of customers or employees), triangulation or loyalty fraud**. Additionally, it improves accuracy and reduces the system's response time to new attack patterns and trends. ML also facilitates real-time decision-making by rapidly evaluating large amounts of transactional data, eliminating time-consuming manual interaction and, therefore, enabling a significant reduction in fraud management costs. **Blockchain or Distributed Ledger Technology (DLT) also promises future benefits for fraud prevention. Let's imagine the application of this highly secure technology for identity management, certification and smart contracts**.

Forewarned is forearmed – what airlines need

The third trend is **Strong Customer Authentication (SCA)**, which **aims to reduce the risk of fraud** and, therefore, increase legitimate sales. SCA requires at least two independent elements among three different categories (something the user *knows*, such as a password or Personal Identification Number (PIN); something the user *has*, such as a smartphone or chip card; and something the user *is*, such as a fingerprint or facial recognition). By increasing the number of steps required at the expense of creating user friction, it could potentially negatively impact sales conversion. In the European Union (EU), the PSD2 regulation aims primarily to protect consumers, which might make it more palatable to them. But it is also important to consider how to alleviate the impact on the client and avoid deteriorating customer experience. Some exceptions are allowed, low risk payments under EUR 30, subscription or recurrent payments or white-listed merchants identified by consumers.

Knowledge

Password

Passphrase

Sequence

Secret fact

Pin

Possesion

Smart card

Mobile phone

Wearable device

Token

Badge

Inherence

Facial features

Fingerprint

Iris format

DNA signature

Voice patterns

Forewarned is forearmed – what airlines need

In parallel, the international card schemes (Mastercard and Visa (EMV)) have introduced 3DS or 3DS 2.0, which is also compulsory. The updated 3DS EMV version supports mobile payment and improves customer experience by reducing the friction generated by the extra steps it takes for the issuer to authenticate the card holder. Gaining ground, mobile payment wallets use the powerful authentication capabilities of the cell phone (fingerprint reader, facial recognition) to secure the payment transaction. And they reduce friction by storing securely the customer's payment details, thus removing all need to enter them manually.

According to McKinsey[16], the impact of such new techniques is significant. Companies using them report a 15-20% improvement in fraud detection, a 20-50% reduction in false positives, and a 1-2 point increase in customer satisfaction. Such measures can be an attractive proposition, opening the way for investment. Airlines should however bear in mind that fraud, like all crime, is an ongoing campaign. Fraudsters adapt to every new challenge and wins on the side of the good guys are short-lived. Investment therefore needs to be ongoing.

[16] McKinsey: Fraud Management: Recovering value through next-generation solutions ↗

How IATA supports the airline industry to win the battle

↓

How IATA supports the airline industry to win the battle

A notable feature of fraud prevention is its collegial nature. Like superheroes, joining forces will result in significant efficiency gains. IATA provides support to the airlines across various working groups, events and activities.

Global Airport Action Days: International collaboration among airlines, travel agents, airports and international law enforcement authorities

The Global Airport Action Days (GAAD) is an activity that results in arrests and investigations of fraudsters. This concerted effort involves representatives from IATA, online travel agencies, payment card companies and Perseuss, as well as airlines and the international law enforcement authorities such as Europol, Interpol, and Ameripol[17]. In the case of fraud, pooling understanding and joint actions, are the only ways an industry can successfully combat it. Collaboration is required to face the network of fraudsters.

IATA Fraud Prevention

Global Fraud Prevention Event

Fraud Prevention Groups

Best Practices Guides

Fraud Industry Sizing

Regional Fraud Groups

Perseuss FraudChasers Event

Global Airport Action Days

[17] Europol press release ↗

How IATA supports the airline industry to win the battle

IATA Events: Global Fraud Prevention Event and other forums

IATA Global Fraud Prevention Event is a two-day annual symposium, occurring in conjunction IATA's World Financial Symposium (WFS) every year. It brings together airlines, travel agents and Online Travel Agents (OTAs), card schemes, service providers and law enforcement agencies from all regions of the world to share the latest payment legislation developments and industry solutions that will impact the way fraud prevention is carried out. IATA is well placed to steer such industry initiatives, and expert at developing resolutions and recommended practices. Industry standards simplify common processes, reduce cost and complexity, encourage innovation and assist airlines in providing a better experience for customers. And they allow airlines to work seamlessly with each other and with other stakeholders such as travel agents, airports, and governments. Holistic fraud prevention should be no exception, but the rule.

There are also airline industry regional forums, which IATA supports, in Europe, Latin America and Asia Pacific, the Middle East, and Africa, and which meet at least once a year. FraudChasers is an online secure forum organized by Perseuss↗, an IATA partner. It brings together fraud analysts from airlines and OTAs.

Request participation by contacting
→ cardservices@iata.org

**IATA
WORLD
FINANCIAL
SYMPOSIUM**

**IATA
GLOBAL
FRAUD
PREVENTION**

How IATA supports the airline industry to win the battle

IATA Fraud Prevention Working Groups: Payment Fraud and Frequent Flyer Fraud

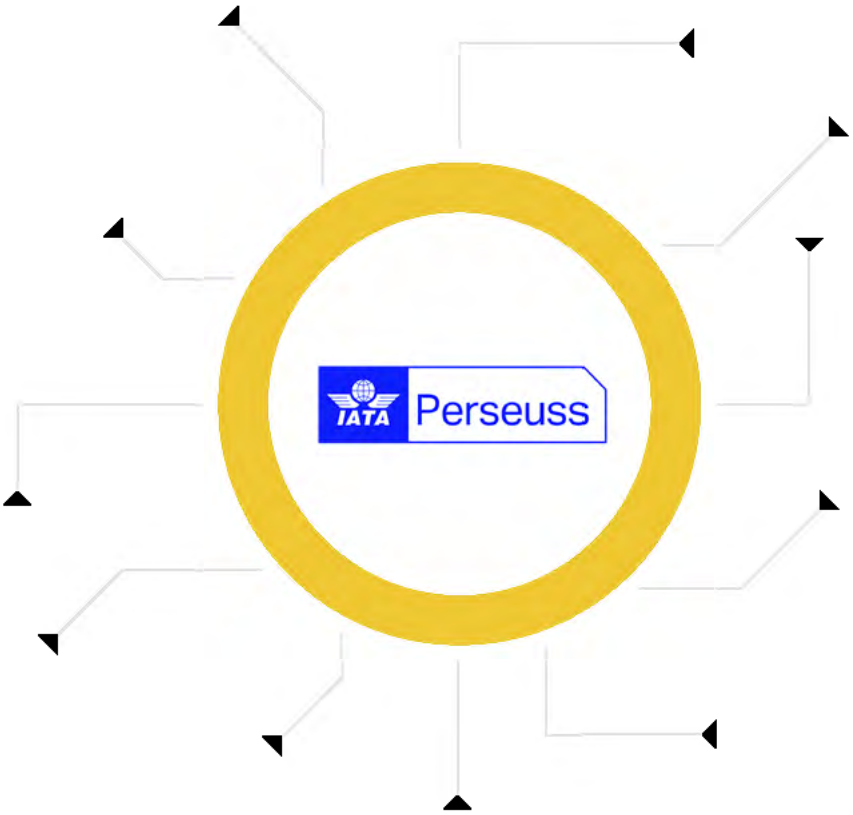
Fraud Prevention Groups for Payment Fraud and Frequent Flyer Programs – acting under the Pay-Account Standards Board↗, one of the five Management Boards that ultimately report to the IATA Passenger Standards Conference – have developed Fraud Prevention Best Practices (FP BP) Guides, for airlines. These guides are a true industry-collaborative effort, with many airlines from around the world contributing to each of them. Covering all the major aspects of payment-fraud and loyalty-fraud prevention respectively, they are updated on a continual basis.

Request IATA recommended best practices by contacting

→ cardservices@iata.org

IATA Perseuss

IATA Perseuss is a leading platform for fraud intelligence, allowing airlines and other merchants to cooperate to identify and fight fraudulent schemes. IATA Perseuss enables real-time access to cross-sector fraud data, through community based sharing between stakeholders in the commercial and payment industry. As fraudsters don't limit their activities to one industry or region, there's an average fraud overlap of 35% between merchants. By cooperating and learning from each other, industry can decrease fraudulent transactions.



How IATA supports the airline industry to win the battle

Industry cost of distribution and payment modelling: sizing fraud impact

Additionally, in 2019, IATA received a new strategic mandate from its Board of Governors. This strategy was articulated around ten strategic streams, covering aspects from digital transformation to environment. **Stream 7, "Airline Efficient Process" scope consists in helping the industry to reduce its cost of distribution and payment**. Following goals have been established:

2022
3% airline unit cost reduction vs. 2017

2035
30% airline unit cost reduction vs. 2017

Therefore, under the Financial Advisory Council (FinAC), **IATA received the mandate to estimate recurrently the size of cost of distribution and payment acceptance**. In collaboration with the Payment Method Working Group (PMWG), IATA has identified what concepts to include in such study. **In the area of payments, these cover payment processing fees, fraud and defaults and treasury management**. Various industry groups, including those dedicated to Fraud Prevention have agreed on the metrics and collection of data methodology.

COVID-19 crisis has put temporarily on hold these undertakings. IATA has reviewed priorities to support the industry during these challenging times. In this regard IATA's focus in 2020 is on three Emergency Priorities improving airlines' liquidity, reducing their costs and preparing the industry for activity restart. **Airlines' tight cost control remains more relevant than ever**. IATA expects to resume this work very soon and is open to include any airline wishing to contribute.

Airlines wishing to participate, please contact IATA at
→ cardservices@iata.org

The industry can rise to new heights

Imagine a world in which all industry stakeholders would share intelligence on cyber-security and fraud challenges across our industry. And not just challenges but also details on existing solutions. Where none are readily identified, all actors work together to identify them and, when needed and possible, develop then in a faster and more cost effective way than anyone could do on their own whether at the passenger transaction level or the agent level. IATA could also assist the industry by developing relevant tools to help relevant stakeholders address payment and frequent flyer fraud risks.

Let’s keep imagining! Innovative smart new contracts, governing a particular transaction with any travel actor, can stipulate the preferred payment method, fraud levels suspected or specifying that it be made at a specific date to encourage the transaction and control costs. For example, using dynamic offering in distribution with payment and fraud prevention could potentially be a win-win-win proposition, providing a safe, fast and cost-efficient cash collection for the airline, while agents (and ultimately the traveling customer) could benefit from a lower fare or other benefits.

The travel industry must secure a place and act now and decisively by offering innovative and cost-effective fraud approaches that meet customers’ needs, but also support the industry to face current COVID-19 crisis challenges.

Subscribe to IATA Air Pulse
to learn more with future
publications on payments.

→

www.iata.org/airpulse