Managing payment card fraud
A guide for airlines

March 2014
Contents

1 Owning up to the airline industry’s card fraud problem
   Visa Europe – a near real time view of fraud
   Some fraud metrics – for context with your own numbers
   Digging deeper – fraud losses by channel
   Card present versus card not present (Visa fraud acquired in Europe)
   Digging deeper – fraud losses by geography
   Digging deeper – understanding the nature of card not present (CNP) losses
   Typical attitudes to fraud – for context with your own business
   Categories of fraud in the airline sector
   Characteristics of fraud in the airline sector
   Visa Europe compliance programmes

2 What could your business be doing better?
   How can you assess the extent of your own fraud problem?
   How can you work more effectively with your partners?
   Make full use of ‘card present’ capabilities and controls
   Get the message across to your passengers
   Using the data that you have – or can easily access
   Fraud detection systems and management
   Fraud topology
   Management information and reporting
   How can the payment system help you reduce your fraud footprint?
   How Visa Europe can help you further

3 Closing thoughts

Appendix
Case study – airline Day of Action
Introduction

This guide looks at card fraud characteristics in the airline industry. In putting it together, we have drawn on our experience of working with individual airlines, and also our engagement with the International Air Transport Association (IATA).

Why have we produced a guide specifically for airlines?

The unfortunate fact is that, for a host of reasons, airlines do generate conspicuously high levels of card fraud.

Visa Europe has a unique place in the value chain – between issuers, acquirers, member/merchant agents, industry bodies and others. With this ‘holistic’ view, we’re ideally placed to work with the airline industry to help reduce the level of card fraud.

• In Part 1, we provide an overview of fraud in your sector – and the reasons you may want to take a harder line within your own business.

• In Part 2, we offer up some suggestions on how you could maximise card acceptance sales, whilst minimising overall operational costs and fraud.

The appendix includes a short case study regarding an ‘airline Day of Action’ which was led by Visa Europe and took place in June 2013. The purpose of this activity was to assess our joint ability to prevent airline fraud by disrupting criminal activity. The airline Day of Action identified more than 200 suspicious transactions, led to 120 arrests so far (as at March 2014) for airline fraud and other crimes for which airline travel was only a part.

We think you will find the summary interesting, as it hints not just at the level of crime being attempted against the airline business, but also the opportunities to address it.

This is the first time that Visa Europe has produced a guide in quite this format – we want it to be both thought provoking and practical.

Our overriding thesis is this: if you were to manage card fraud more actively, you could eliminate a layer of unnecessary cost from your business and avoid some formidable reputational risks – with no adverse impact on the experience of your legitimate customers.

I hope you find the guide useful. But, if you have any thoughts or suggestions for future updates, please do let me know.

Peter Bayley
Executive Director, Risk Management, Visa Europe

Email: fraudmanagement@visa.com
Part 1

Owning up to the airline industry’s card fraud problem

In this part of the document we consider the level and nature of card fraud in the airline sector — and the reasons why it is disproportionately high.
Visa Europe – a near real time view of fraud

Visa enables cardholders and merchants to transact, easily and spontaneously, anywhere across the globe.

Under Visa rules, every card issuer is obliged to investigate every occasion in which a cardholder claims a transaction has been undertaken without their permission.

The issuer must investigate the cardholder’s claim. If they accept that fraud appears to have occurred, they are then required to send Visa what is known as a TC40 message advising the details of the fraud.

Visa collates and validates these TC40 messages, and rejects those that do not meet minimum standards.

TC40s are then used to:

- Support investments in new systems and infrastructures
- Support changes in business models
- Maintain and operate appropriate compliance programmes
- Update the Visa Europe Board on fraud performance
- Determine priorities for Visa Europe

TC40s are not a perfect expression of fraud losses, but they are integral to the way the payment scheme operates. They are also vital in ensuring that Visa Europe maintains its disciplined focus on:

- Minimising fraud to all parties in the payment system
- Enabling cardholders and merchants to benefit from the best possible transaction approval rates
- Reducing costs of fraud risk management incurred by all parties to as low a point as possible
- Identifying and highlighting fraud patterns

In this light, let’s look at what the fraud numbers currently tell us about fraud performance in Europe.
Some fraud metrics – for context with your own numbers

In Visa Europe, fraud is a core business metric.

As of September 2013, our overall fraud rate was 4.5 basis points (expressed another way, fraud losses equate to 0.045% of total sales, or €0.045 in every €100 of spend) on a Visa card.

This performance reflects the focus and investments made by all payment system parties over the 50-plus years that Visa has existed.

The levels of fraud differ, according to the channel in which the transaction occurs, and also the merchant sector.

As a whole, the airline industry does not compare well with other merchants operating in the Travel & Entertainment sectors.

At the very best performing airlines, we see fraud rates of less than six basis points, but, for most airlines, the rates tend to be much higher, particularly through the unsecure e-commerce channel.

And, at two of Europe’s ‘flag carrying’ airlines, we have recently seen fraud rates in excess of 60 basis points – which is around 13 times higher than the Visa overall average.

These levels of fraud are unsustainable. They are not good for our business, and it is difficult to believe that they are good for yours either.

Digging deeper – fraud losses by channel

For face-to-face or ‘card present’ transactions, fraud levels are below four basis points. This is because most Visa Europe transactions are now protected by Chip and PIN – with the powerful cryptography inherent in Chip transactions providing very strong security, and the use of a PIN providing an extra layer of defence.

As more countries in the world migrate to Chip and PIN technology, we expect to see the ‘card present’ fraud rates being pushed progressively lower. But, when transactions are conducted over the telephone or on the internet the scope for fraud increases significantly.
Card present versus card not present
(Visa fraud acquired in Europe)

<table>
<thead>
<tr>
<th>Visa Europe fraud rates</th>
<th>All fraud for year to Sep 2013</th>
<th>Airline fraud for year to Sep 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Present</td>
<td>3 bps</td>
<td>54.2 bps</td>
</tr>
<tr>
<td>Card Not Present</td>
<td>20 bps</td>
<td>27.7 bps</td>
</tr>
</tbody>
</table>

The airline fraud performance through CNP, a predominant and growing channel, is not significantly higher than the overall Visa CNP fraud rate. However, serious consideration should be given to what more could be done to bring card not present fraud rates down from 27 basis points to more acceptable levels.

What is it about the airline industry that allows card present fraud rates of 54 basis points, in a market where Chip and PIN acceptance provides such an effective counter-measure driving an 18 times lower fraud rate? Although card present accounts for a small minority of total sales, the related fraud losses are disproportionately high and should be relatively easy to manage downwards.

We would suggest that, if your own business runs anywhere close to these industry averages, both card present and card not present fraud deserves your urgent attention.

Within this guide, we hope to provide some pragmatic solutions and actionable insights.
Digging deeper – fraud losses by geography

Another way of looking at fraud is to consider the location of your customers (and the country in which their Visa card has been issued). We appreciate it requires a little bit of work to do this, so Visa Europe is looking into whether it can deliver a service that will make it much easier – thus enhancing your risk management decision making processes.

It is useful to understand that different issuer markets contribute different levels of fraud to the airline business, with different underlying rates. If we look at the total fraud incurred by airlines for the year to September 2013, we can see the main issuer percentage split based on the country where the card was issued:

<table>
<thead>
<tr>
<th>Market</th>
<th>% of Visa Europe Airline fraud</th>
<th>Fraud rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>19.3%</td>
<td>126 bps</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>16.0%</td>
<td>12 bps</td>
</tr>
<tr>
<td>France</td>
<td>15.4%</td>
<td>48 bps</td>
</tr>
<tr>
<td>Canada</td>
<td>5.5%</td>
<td>190 bps</td>
</tr>
<tr>
<td>Germany</td>
<td>5.1%</td>
<td>29 bps</td>
</tr>
</tbody>
</table>

Ascertaining the location of customers is not conclusive. If 80 per cent of all of your sales were to UK-based cardholders, you wouldn’t be surprised if the majority of your fraud also emanated from the UK. As a general principle though, there are higher risks associated with the distance a cardholder is from their home location and needs to be considered as part of any risk-based decisioning.

Different markets see different rates

There are higher risks associated with the distance a cardholder is from their home location – this needs to be considered as part of any risk-based decisioning.
Digging deeper – understanding the nature of card not present (CNP) losses

For most airlines, CNP has become by far the largest payment channel – and, given the inherent risks of CNP transactions, it is worth looking at the related losses in particular detail.

By doing so, we can break down fraud type by three further categories. This helps us to understand how risk differs, based on the way airlines and their partners process their transactions.

These categories are:

**MOTO** (which is shorthand for Mail Order, Telephone Order and Recurring Transactions) – typically transactions originated by a cardholder speaking to the merchant over the telephone.

**Secure Electronic Commerce** – typically transactions processed over the internet that have benefited from the use of Verified by Visa (VbV) using the 3D Secure protocol.

**Unsecure Electronic Commerce** – an internet transaction that has not benefited from a VbV validation. (See also page 22)

If we look at fraud performance at this level of granularity, we see the following overall performance during the year ending September 2013:

<table>
<thead>
<tr>
<th>Acquired CNP channel</th>
<th>% of Visa Europe airline fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail/Telephone order (MOTO)</td>
<td>32%</td>
</tr>
<tr>
<td>Secure e-commerce (VbV)</td>
<td>14%</td>
</tr>
<tr>
<td>Unsecure e-commerce</td>
<td>54%</td>
</tr>
</tbody>
</table>

As you can see, the majority of CNP loss occurs through unsecure channels and most of this is unsecure e-commerce. It is also notable that the underlying fraud rate within VbV secured transactions is far lower than the unsecure channels. A merchant that supports VbV can normally expect a full payment guarantee in the event of fraud (although liabilities do remain for service failures, product defects and so on).

You can appreciate therefore, why Visa Europe has been a strong advocate of VbV. The lower fraud rate and fraud guarantee offer a massive opportunity to merchants, whilst also taking significant cost and inconvenience out of payments for the other payment stakeholders.

Many airlines we have spoken to do raise concerns about the impact that VbV may have on the customer experience. But what many businesses don’t realise is that VbV can be used selectively. For those transactions that are most prone to fraud, it can be automatically deployed. For those that are deemed, by your own organisation, to be lower risk, it need not be invoked at all.

It should also be noted that many issuers have implemented Adaptive Authentication, which means that the number of authorisations that go through the full VbV authentication process has reduced significantly – leading to an improved experience for cardholders and reduced drop out rates for merchants.
As an airline, what is an acceptable level of fraud to you? How does your fraud rate compare to the above figures? Given the high level of fraud incurred amongst airlines, the Visa Europe fraud teams have been actively engaging with their counterparts in the sector.

We have partnered with IATA and participated in a number of industry-level initiatives. We have also worked with individual airlines to understand their respective business models, identify their fraud drivers, and seek opportunities to improve their performance.

Through this work, we have identified a number of industry characteristics. And, again, it may be useful to compare these norms with your own business. Although there are some notable exceptions, here’s what we have found:

• **A high tolerance to fraud**
  
  Due to the nature of the service being sold, many airlines have a higher tolerance to fraud than many other sectors (for example, a jeweller selling an intrinsically valuable gold ring will have a very different attitude to card fraud than an airline selling a seat that may otherwise remain empty). And, when airline load factors are low, this tolerance to fraud tends to rise accordingly.

  This high tolerance to fraud within some airlines is, in our experience, a misjudgement. The assumption appears to be that the marginal cost of potential fraud on an airline flight which may not have full occupancy is an acceptable business risk. But often tickets end up being utilised on partner airlines where real money changes hands or on popular flights where a genuine sale could have been achieved.

  Allowing fraudsters to travel also leads to secondary losses as well; the fraudulent in flight sales can often represent significant additional losses and chargebacks.

  But perhaps the biggest risk is simply that of allowing a fraudster to fly (whether on a bad card or via a late cash payment). If he/she was prepared to commit card fraud to board one of your flights, how likely is it that they are involved in, or prepared to support, other types of crime?

In fact, from our dealings with airlines and law enforcement, we have seen what appears to be a strong correlation between card fraud and other crimes including people and drug trafficking, terrorism and immigration offences.

What could it mean to you as an airline in terms of potential reputational damage and/or regulator action if it became public knowledge that a traveller involved in a serious criminal incident could have been identified and prevented, based on some straightforward financial controls?

Is the benefit of some minor revenues really worth the wider PR and regulatory risks that this could create?

• **Cooperation with other stakeholders**

  There are airline fraud prevention groups who do work closely to mitigate fraud and their lobbying delivered the IATA Perseuss anti-fraud database. However there is always room for improvement in terms of cross-industry dialogue and collaboration (but respecting concerns over data privacy) and engagement directly with the payments industry. This was clearly demonstrated by an exercise carried out in the summer of 2013 and co-ordinated by Visa Europe. This involved the airlines, card issuers and law enforcement agencies in a day of action to identify and act upon fraud and has so far led to more than 120 arrests (as at March 2014). These were not just for payment crime – there were clear links to other serious crimes as mentioned previously, clearly demonstrating the value of cross industry collaboration. For more information, please see the case study at the end of this document.

• **Limited cooperation with the authorities**

  There is also very little dialogue with law enforcement agencies (mainly brought about by challenges surrounding jurisdiction). As a result, these agencies are not fully aware of the nature or the extent of payment card fraud in the airline sector, and are rarely (if ever) called when fraud has been detected.
• **Complex relationships with Global Distribution Systems (GDS)**

Another clear issue is the complex nature of the relationships with the GDS, and their Billing Settlement Plans (BSP) which most airlines and travel agents rely on for reservation, ticketing and payment services. Whilst we accept that these relationships are sometimes intricate and add a level of complexity to airline transactions that we do not see in other sectors, there are some opportunities we believe should be explored.

The specifics will differ from airline to airline and GDS to GDS. But a typical issue is the elapsed time between a reservation being made via the GDS and the settlement for each airline transaction that operates through IATA’s BSP. The BSP manages the transmission of the file to the acquirer for settlement or sends it to the airline to pass on to the acquirer (often this period can exceed ten days – by which time the fraud has been successfully perpetrated, the ticket utilised and the passenger has flown).

If there is any way that the processes between you, your GDS and IATA’s BSP can be made more efficient to ensure a faster exchange of information, we encourage you to make those changes.

We know that IATA continues to look at ways of improving the shared infrastructure at airports to provide Chip and PIN functionality. We therefore recommend that you give this your support, particularly in light of the very high card present fraud rates mentioned earlier in this document. Our view is that card present fraud levels in the non-Chip environment will only increase. If it is not a problem for you today, it will be shortly.

In the e-commerce space, VbV should be used wherever possible as the secured channel delivers a significantly better fraud performance. If you are not using VbV through your direct sales, seriously consider whether this is right. If your GDS is not using VbV, consider whether outsourcing this activity is the right thing to do.

Clearly every business will have its own particular risk appetite, and will generally take account of:

- Initial losses (in terms of chargebacks)
- Secondary losses (in terms of subsequent fraudulent transactions)
- Associated operational costs
- The reputational implications
- The regulatory implications

Our experience at Visa Europe is that the true implications of card fraud for airlines are often overlooked or underestimated. Fraudulent ticket sales tend to lead to further high value fraudulent transactions.

The fact is that, with some basic controls, much of this cost and risk could be eliminated – with no negative impact on either legitimate revenues or the customer experience.

---

**Potential reputational damage and/or regulator action**

What could it mean to your airline in terms of potential reputational damage and/or regulator action if it became public knowledge that a traveller involved in a serious criminal incident could have been identified and prevented, based on some straightforward financial controls?
Categories of fraud in the airline sector

Based on the work we have undertaken, we have identified five broad categories of fraud in the airline sector relating to card payments, namely:

- **Fraud flyer** – tickets are fraudulently purchased by an individual or group with the intent to travel (and may do so using either genuine or fraudulent documentation). This is card fraud at its simplest as the fraudster(s) are buying tickets for their own use.

- **Card checker** – a transaction is attempted to test the validity of compromised card and personal data (in support of the on-selling of this data to other criminals). It is likely that the transaction does not complete, and if it does it may be cancelled or simply never used. The fraudster is using your systems to check card status – but if the transaction goes through it still represents lost revenue and a risk of liability.

- **Fraud agent** – a ticketing scam in which a ticket is bought fraudulently and then re-sold, usually to an innocent or unsuspecting traveller. Whilst it is tempting to feel sorry for the ‘genuine’ traveller, they are probably aware that the deal is unbelievably good and the only way to stop these scams is to create problems for the ultimate customer. Effectively, because the payment was fraudulent, the ‘customer’ does not hold a valid ticket. As a minimum they should not be permitted to fly.

- **Airside access** – tickets are fraudulently purchased, not because anyone intends to fly, but because criminals want to go airside in order to steal from an airport’s duty free shops.

  This is a problem specific to airports where incoming passengers mix with those waiting to travel and airlines should be conscious of this problem at affected airports.

- **Policy fraud** – first party fraud, usually relating to travel upgrades or excess baggage costs. Checking of the card details against the travellers’ passport and boarding pass would help to eliminate this type of fraud. Support of Chip and PIN for changes in value would help even more.

- **In flight sales** – without the ability to on-line authorise transactions in-flight, fraudsters exploit this using compromised cards that may or may not have been used to purchase the ticket to fly. Give some thought to changing the process here and check credit/debit cards to the passenger’s passport and boarding cards when they make a purchase. Ideally record the details of the passport (i.e. date of issue, number and issuing authority) for future reference.

Airline fraud departments should be aware of these categories of fraud, and have mitigation measures in place.

It is accepted that telling a fraud agent purchase from a fraud flyer can be difficult.

There is a fraud problem specific to airports where incoming passengers mix with those waiting to travel.
Characteristics of fraud in the airline sector

Through engagement with the industry, we see a number of characteristics that often apply to fraudulent transactions. This does not mean that all fraudulent transactions meet these criteria or that all payments which meet these criteria are fraudulent. But they were sufficiently relevant for the airlines we have spoken to to warrant summarising here:

- Tickets that are purchased close to the departure date (often within 48 hours)
- It is not unusual for tickets to be changed or amended close to the departure time (for example, changes to the departure or destination)
- Tickets are often for return flights or stop-over routes, but only the first leg of the journey is completed
- Tickets are often purchased during the early hours of the morning
- Tickets seem to often be for high occupancy flights
- Multiple tickets and travellers are often associated with a single card transaction

There tend not to be any real commonalities between the sex, age or nationality of people travelling on fraudulent tickets. Also the class of ticket and the route seem to be irrelevant.

Later in the guide we suggest some ways in which you can correlate payment industry data (in the form of TC40s) with your own data to help identify the type of transactions which are most prone to fraud within your own business.
Visa Europe compliance programmes

As demonstrated above, Visa Europe understands that the risk associated with a given card portfolio or merchant sector differs, and we expect that fraud rates will differ between stakeholders as a result.

However, Visa Europe also passionately believes that reducing fraud to all stakeholders is in the best interests of all parties and society as a whole. We therefore run a series of fraud compliance programmes – to identify entities with disproportionately high levels of fraud, and to create incentives for them to reduce the fraud they generate.

These programmes currently focus upon issuer, acquirer and merchant excess levels of fraud across the payment system.

The programmes all operate at least monthly and entail financial penalties and/or liability changes for those entities with high fraud trends.

Please note that Visa Europe also operates several other compliance programmes which are not fraud-related.

As a merchant, your acquirer should work with you to maintain a low fraud threshold, but will advise you if you are ever reported within a Visa fraud compliance programme – thereby enabling you to take joint action to avoid or address the fraud issue. The closer you work with your acquirer in these circumstances the better. The ability to demonstrate that appropriate and measurable actions are planned or have been implemented to address excessive fraud and/or chargebacks will be beneficial.

Regardless of this, one should always remember that all fraud results in a real cost to your business, and that the management of these costs within acceptable levels is the key focus for a fraud manager.
Part 2

What could your business be doing better?

In this part of the document, we consider some basic steps that your own business could be taking to cut down on the costs of card fraud – as well as the wider risks.
How can you assess the extent of your fraud problem?

Understanding the level of fraud being incurred as a result of your sales, whether very high or very low, is a critical part of a merchant fraud manager’s job.

Merchant fraud managers will often focus on chargebacks as the problem that they are looking to address, as these represent a direct profit and loss impact. Whilst this is a critical measure, there is arguably an equally useful one.

The TC40s that issuers report to Visa each day are also made available to your acquirer – although they may charge a small fee for extracting and providing them to you.

Taking these TC40s as the overall fraud number when managing your business is important, as they have certain significant benefits:

1. They represent all of the fraudulent transactions reported by issuers to Visa – and not just those that the issuer has charged back.

   This allows you to identify which of your customers are processing transactions with you as fraud (if you don’t mark them as fraud now, they may come back for more, and the issuer may well chargeback).

2. They contain all of the details of which cards, from which issuers and in which markets are experiencing fraud.

   For detection purposes, you want to know which issuers, in which countries are creating most of the fraud for you. This could enable you to minimise the associated losses. It could also enable you to be more lenient with those issuers and countries that do not pose a high risk.

3. The TC40 fraud records are delivered much more quickly than chargebacks, and are sent to your acquirer every day.

   As such, you know about fraud earlier – you can see changing trends earlier, you can block repeat business earlier, and you may even be able to stop a passenger from checking in on those transactions that slipped through the net.

   This can be particularly useful for ticket sales that originate from the GDS, given the time it takes for you to receive clearing records.

4. This provides you with an overall measure to track your performance over time – in the same way that Visa and your acquirer will track you.

   This means that, if your fraud rate is deteriorating, you will know about it as quickly as Visa does. You can see how your performance is improving or deteriorating, test strategies and know your overall fraud rates.

If you don’t have access to TC40s please speak to your acquirer about how you can receive them. If your acquirer cannot help you, please email Visa Europe at fraudmanagement@visa.com. We will aim to put an appropriate reporting process in place, albeit for a small fee.
How can you work more effectively with your partners?

As we acknowledge elsewhere in this guide, the complexity of the relationships between airlines and their partners (primarily GDS and travel agents) can create certain blind spots – which become a breeding ground for fraud.

Irrespective of who may be liable for any losses through both the normal chargeback process or any fees that may result from a breach of Visa Europe’s compliance programmes (you the airline, the GDS, a travel agent, or even the card issuer), it makes sound commercial and reputational sense to minimise the level of fraud that does occur – and for all stakeholders to work together in order to do so.

It is also worthwhile checking your contractual terms with partners – whilst it may be possible to pass on chargebacks, you are probably unable to pass on scheme compliance fees.

We would therefore urge you to work very closely with your partners to establish fraud management and mitigation programmes. It is our experience that seemingly small changes can have a big impact on fraud detection and, ultimately, fraud prevention. Such opportunities include:

- Implementing real-time or expedited access to authorisations
- Improving the speed of data delivery
- Sharing and acting on your respective insights into fraud, where it’s occurring, when it takes place and who is doing it.

By working together and sharing data, it becomes much easier to identify and analyse fraud patterns – for example, by isolating high-risk routes, via what destinations, from which agents, IP addresses, account numbers, booking times and so on. Getting the data is key to everything else.

Also, as a customer, you can put pressure on your business partners to invest in and make use of fraud prevention technologies (including the use of relatively simple measures such as Chip and PIN-enabled point of sale terminals). Some GDS are looking at how to improve their risk management processes and may have options available to you – engage with them and determine how you can work together to take risk out of the system.

Where you spot a high risk transaction – what processes do you have to manage the individual who turns up with an invalid ticket? Some airlines simply cancel the transaction and ask for cash, thereby exposing themselves to further fraud loss in-air and as tickets are changed later in the route – as well as to the risks associated with smuggling, fraudulent documents and other criminal activity. Why take these risks?

As such:

- What process do you have in place for your staff to handle referrals?
- How do you ensure the job they do is appropriate and effective?
- What metrics do you monitor?

Some Global Distribution Systems are looking at how to improve their risk management processes and may have options available to you – engage with them and determine how you can work together to take risk out of the system.
Make full use of ‘card present’ capabilities and controls

There is no logical reason why airlines should be experiencing excessive card present fraud losses.

In the 21st century, there is no excuse for any business to generate (or fall victim to) high levels of keyed transactions (in which card details are manually entered into a terminal), or mag-stripe read customer present transactions in which card details from a magnetic stripe have been incompletely or incorrectly read.

And, as card issuers in more and more countries migrate to Chip and PIN, any remaining pockets of magnetic stripe acceptance will be increasingly targeted by criminals.

As such you and your partners should be doing all you can to implement Chip and PIN-enabled card acceptance devices – if only to benefit from the related liability protection.

If, for whatever reason, your GDS or travel agency partners are unwilling or unable to invest in the related devices and technology, you should be doing so across your own business – including all check-in desks, sales counters and in-flight acceptance devices.

If you have not already done so you should also be talking to your acquirers about the opportunities for developing online authorisation of your in-flight transactions.

The related fraud rates for in-flight transactions can be very high. Criminals will actively target high-value goods that can be sold-on. And, as highlighted elsewhere in this guide, there is a very strong correlation between fraudulently purchased air tickets and fraudulent in-flight transactions. Visa Europe would support any airline that would be prepared to trial the matching of passports to the proffered card for in-flight transactions to reduce the risk of fraud.

We would also recommend that you discuss with your acquirers whether, through what can be complex business models across multiple locations and geographies, you are maximising the benefits of secure Chip and PIN and VbV authenticated transactions – particularly where you are outsourcing some or all of your processing to a third party.

It may be worth checking, potentially with the help of your acquirer, that there is no degradation of the authorisation message between you, your partner, the acquirer and the issuer that downgrades a Chip and PIN or VbV authenticated transaction from the highest form of security. You may find that a small change to your processing model delivers huge benefits.
Get the message across to your passengers

One very easy way to reduce fraud is to demonstrate to your passengers that you take it very seriously.

For example, you can state clearly on your website and other communication channels that any passengers found to be using a fraudulently purchased ticket will not be allowed to board. You can also display the details of market-specific laws and penalties relating to fraudulent ticket purchases. And you can state that any instances of fraud will be reported to the authorities.

It is our experience that such messaging is reassuring to legitimate passengers, but encourages potential fraudsters to try their luck elsewhere.

Using the data that you have – or can easily access

In our experience, most businesses that trade remotely (irrespective of industry sector) are becoming more adept at isolating and collecting data for fraud purposes.

Positive data helps you to identify passengers who travel frequently and do not generate fraudulent transactions. Meanwhile, negative data helps you to identify those who have previously perpetrated fraud.

For each case, such data could include IP addresses, device profile, passenger names, billing details, mobile phone numbers, email addresses, postcodes, and so on.

In our experience, conscientious fraud managers are also making use of publicly available and easily accessible data, such as social networking profiles and telephone directory entries, to confirm a passenger’s identity and/or legitimacy.

See below for suggestions on how this granularity of data could be incorporated into or used alongside your fraud detection systems.
Fraud detection systems and management

Detection system management is critical to any business involved in payments, including merchants.

Frequently, a failure by a merchant to operate within acceptable fraud and chargeback levels is directly associated with a failure to monitor these elements, combined with the lack of a fraud detection capability.

Within a merchant business, detection is primarily about streaming high and low risk business. This allows you to speedily process sales for the low risk business, reject clear fraud activity and isolate – for manual review - any higher risk, but less obviously fraudulent, transactions.

It is not possible in this space to discuss detection in detail. However, any effective detection systems will typically include:

1. A data selection area – what data can you make available to your system in order for it to assess risk?
2. A negative database (developed in-house or sourced externally) of known fraud and related characteristics.
3. A positive database of known excellent or undoubted customers.
4. A statistical model (scorecard, neural network or similar – it doesn’t really matter which type it is, as long as it is statistically based and you understand the performance). This allows you to risk score transactions based on known consumer profile such as order history, purchase velocity, device tracing (geo-location, fingerprinting) and previous fraud experience.
5. A rules system that allows you to use the above elements to create relevant business strategies (this is not a replacement to the statistical model, but an important addition).
6. An uplift mechanism – what are you going to do with the high risk transactions? This could be a referral into an operational area or uplift to a different processing approach.

Having created these elements, you will also need to monitor how effective your fraud detection system is at managing fraud loss.

Using TC40 (and chargeback data as this will show a slightly different but equally relevant performance), you can then calculate the core fraud detection metrics:

1. **Value detection rate**
   Of all of the fraud occurring through your sales channels, how much did your system actually detect (you then have a separate view as to whether you took the optimal action).

2. **False positive rate**
   For every alert or uplift your system created, how many transactions do you believe were definitely fraudulent (if the transaction proceeded and you have a TC40 or a chargeback, then you have a clear understanding – if not, you have to have some very honest criteria to assess this).

3. **Customer impact**
   How many of your customer transactions are you negatively impacting with your detection system – be that a delay in despatch, further questions or validations before the sale proceeds, or manual reviews.

This leaves you with a series of metrics that allow you to justifiably argue your detection performance versus business impact.

If you detect (say) 50 per cent of all the fraud hitting your sales portal, with

i. A false positive rate of (say) 1:7 (i.e. for every fraudulent transaction that you stop, you review seven genuine transactions)

ii. And a customer impact of (say) 5 per cent (i.e. 95 per cent of your transactions are going through the system clean and only five per cent needs some special or manual process)

Then you can sensibly discuss with your wider business how well you are doing and whether you need to tighten or loosen controls.

What’s more, you can also track performance over time to see whether your system is improving or deteriorating.
Fraud topology

There are various ways in which a detection system could be configured, but a summary of a logical, albeit slightly simplified, approach would be as follows:

This topology shows an approach in which a (VbV-capable) merchant is using both a statistical model and rules system, supporting a grey list and a white list.

The grey list would include, for example, known bad customer addresses, names, devices which you would always look to refer for review with a probability that you will decline. The white list would include the converse – customers you know are valuable and you would like to process regardless of what or how they are buying (although, even for these, a limit on spend would be sensible).

The statistical model will provide an easy way for you to optimise your rules, providing better fraud detection performance and customer experience – a difficult balance to achieve.

The rules then enable your fraud staff to add their expertise and knowledge.

In this instance, VbV (3D Secure) is being used as the uplift for the higher risk activity, albeit increasingly merchants will use VbV for all of their traffic because of the wide risk benefits and reducing customer impacts (see the VbV section a little later on). But, even where this is not an available option, you may wish to consider other manual methods or approaches to verifying transactions.
Management information and reporting

A robust management information (MI) pack, which combines current performance and trends, should be critical to everything you do.

Without strong data, reported very regularly (ideally daily and weekly) and showing the core trends in fraud performance, you are like a hunter wearing a blindfold: you can hear the ducks all around you, but hitting one will be a question of luck – and luck is not something a fraud manager ever wishes to rely upon.

Although some of the data may take a while to fully mature, and must always include trend data, your MI pack will provide a daily overview of:

1. Financials and fraud
   - How much fraud am I seeing?
   - What am I seeing in chargebacks? (my P&L impact)
   - What are my net and gross fraud-to-sales ratios?
   - Which issuers, markets, channels and goods are responsible for the fraud?

2. Detection
   - What is my value detection rate, false positive rate and customer impact?
   - What are my lost sales from detection activity?
   - What proportion of lost sales do I believe is fraudulent, and why?
   - What declines am I generating for non-fraud reasons?

3. Operations
   - What are my operational support processes and how well are they working?
   - How many employee hours am I spending on detection and at what cost – by core function?
   - Am I and my third party support areas meeting operational service level agreements?
   - What are the fraud control operational costs to the business?

4. Complaints
   - How many complaints am I receiving, and for what reasons?
   - What other negative outcomes am I creating?
   - What am I doing about them?

5. Wider business impact
   - What impact are my fraud systems having on the wider business – good and bad?

6. Law Enforcement and industry
   - What successes have I had in terms of arrest and prosecution?
   - What industry (including IATA) benefits/opportunities have I realised?

7. Autopsy and change
   - What major losses and service failures have I seen in recent weeks?
   - What were the causes, including staff fraud and staff error?
   - What changes am I making as a result – and what is the status, timeline?

There may be other metrics that are relevant to you, but your MI pack should cover most of the above. Whether you share it all is your call (we think you should), but at the very least, you should be tracking it.
How can the payment system help you reduce your fraud footprint?

In existence for more than 50 years, Visa is a product of constant change, enhancement and evolution.

It was originally designed as a paper-based payment system, allowing for fast and convenient payments for all stakeholders in the traditional brick-and-mortar payment environment. Back then, the internet was the stuff of science fiction, yet Visa has arguably become the core payment solution within the online space.

Throughout this evolution, risk tools have been created to help manage risk within the e-commerce space – and these are continuing to evolve.

But as of today, all merchants should consider the following:

1. **Online authorisation**
   Visa supports and maintains an authorisation system which allows merchants to transact on a fully 24x7x365 basis. The system is almost instantaneous and validates that:
   - The card is not identified as lost, stolen or misused
   - The card details, including any security elements are correct
   - The address of the cardholder is correct (in countries where address verification is supported)
   - Sufficient funds are available on the account

   It also confirms that the issuer is comfortable for the transaction to proceed, based on its own detection systems.

   Merchants engaged in e-commerce are required to authorise all transactions before progressing a Visa payment – and you should never be tempted to skip this, as unauthorised transaction activity will create massive risks to your business.

2. **Verified by Visa (VbV)**
   This has been mentioned previously as part of the detection and topology disciplines. VbV is Visa’s security infrastructure, which allows customer authentication over the internet during a purchase.

   VbV is not an authentication in and of itself, but a mechanism that allows a dialogue between the cardholder and the card issuer so that the card issuer can undertake whatever checks they feel are necessary to identify the customer. Depending on the issuer’s preferences, this can include a password, a partial password, an out-bound SMS or some form of cryptographic token.

   Increasingly issuers are running their own detection systems against VbV authentication messages in order to identify and challenge out-of-character transactions. This means that, on occasions, no direct customer challenge is occurring at all – an approach which maximises customer speed and convenience without reducing security.

   Today, the fraud rates of transactions that are protected by VbV run at less than a quarter of the level experienced by traditional unsecure electronic commerce traffic. Because of this vastly superior fraud performance, merchants will normally benefit from a payment guarantee for fraud if they use VbV.

   As such, any merchant accepting Visa payments over the internet should support VbV, if not for all their payment traffic, at least for some of it.

   Of course, the use of VbV does not remove the merchant’s responsibility for managing fraud risk and detection systems mentioned elsewhere in this paper (i.e. it does not give immunity from compliance programmes). But it can make a huge difference both to the fraud levels incurred and the customer experience offered (which in turn means that compliance programmes should not be breached).
3. Card Verification Value 2 (CVV2)

On the back of every Visa card is a three-digit number, typically part of the signature strip. This number cryptographically ties together the card number (sometimes referred to as the PAN) on the front of the card, together with the expiry date, and allows a simple validation that the data input is correct.

As a security tool, CVV2 is often ridiculed – it sits on the back of every card after all, and is therefore easy to compromise. But it does offer a very valid role in confirming that the card and expiry date are valid.

Visa does not allow the CVV2 to be stored (a stipulation which falls within the PCI DSS requirements). So, if you do not process authorisations immediately (as is the case with some hotels) this may not be available for you to use. However, if you can process it immediately, CVV2 provides a useful hygiene check and one that most cardholders are well accustomed to.

The use of CVV2 by merchants (where it does not conflict with PCI DSS requirements), is actually mandated in Europe, and card issuers are mandated to validate it and decline authorisations if it is wrong.

Visa Europe works hard to minimise the use of CVV2 in other channels (for example, it is not captured at brick and mortar merchants, and is not available through the contactless interface on either a card or a phone). If this type of transaction data were to be compromised, a CNP merchant that uses CVV2 is somewhat insulated.

The simple message is always to use CVV2 if you are able to do so. The Visa Europe rules require use when you can do so securely, and it is a painless way to validate that all other card details are genuine.

4. Address Verification Service (AVS)

The validation of address details is not available for many countries, but it is for Europe’s biggest CNP market, namely the UK. It is also available for some of the larger markets elsewhere in the world, such as Canada and the USA.

The value of AVS differs according to your business model and the need to deliver goods – but validating that the address the customer is providing to you, and confirming that this matches the address to which the issuer is sending their statements, can be a useful additional feature.

The validation is undertaken during the authorisation message.

Other enhancements for e-commerce payments are being developed all the time – the most significant initiative being V.me by Visa, the new digital wallet solution from Visa and leading banks, which is now moving to a phased roll-out.

But for now, Visa Europe does provide a number of tools to help manage risk for merchants. You are not required to use them all, but you should be aware of their availability. You should ensure that, if you are not using them, this is a conscious and validated decision, rather than an accidental default.
How Visa Europe can help you further

If you have any questions or issues arising from this guide, you should contact your acquirer in the first instance. It is an acquirer’s job to work with their customers to help you accept and process payments securely – and to manage any issues that you may have in terms of fraud trends.

In particular your acquirer may be able to help you in the following ways:

• **TC40**
The acquirer receives daily fraud reports from Visa Europe relating to fraud incurred in your business (the TC40 files mentioned above).

They should be able to make these available for you.

• **Risk tools**
Many acquirers maintain risk tools and solutions for their merchants – ask them about what is available, and at what price.

You may be surprised at the resources available to you.

• **Advice and support**
All major acquirers will have their own risk management and chargeback experts – look to engage them to help you minimise the fraud risk you are experiencing.

If your acquirer is unable to help you, then you may wish to consider coming to Visa Europe directly.

Visa Europe also makes available:

• **Fraud reporting and benchmarking**
Our data can help you to track your own performance and understand changes in trends. This data is available in both raw and processed (report/KPI) versions.

• **Risk solutions**
Visa Europe does not currently offer merchant fraud detection solutions, but we do have agreements with major vendors – and we may be able to offer direction and discounts if a merchant has a particular need.

• **Training and consultancy**
Visa Europe is increasingly working with merchants to provide direct training and consultancy services – drawing on the wide range of experience we have gained in offering similar services to issuers and acquirers.

Inevitably, these services are not without some cost, depending on scale, frequency and requirements. But if you have an interest, please drop an email to fraudmanagement@visa.com and we will aim to assist you.
Part 3

Closing thoughts

We hope this guide has provided a useful summary of Visa Europe’s thoughts on how to manage and minimise transaction risks for airlines.

If nothing else, a more active management of fraud could help your business to effectively eliminate an entire layer of unnecessary costs which – for a low margin sector – is perhaps an interesting possibility.

This guide cannot be fully comprehensive and the Visa Europe approach to fraud management will continually evolve – but we hope you found the read interesting.

If the guide has raised any queries – or if it doesn’t include any considerations relating to risk management that you think important, please email fraudmanagement@visa.com and we will look to include this in future versions.
Case study: airline Day of Action – coordinated approach leads to sector-wide collaboration

An inaugural airline fraud working meeting was held in February 2013. Co-chaired by Visa Europe and Europol - the European Union’s law enforcement agency - the meeting was attended by ten airlines and a number of law enforcement representatives. The meeting helped to identify fraud trends, criminal methodologies and criminal groups, and ultimately led to the cross-border Day of Action.

Successful Day of Action
The objective of the Day of Action - which took place on 27 June 2013 - was to prevent airline fraud by disrupting criminal activity. It was supported by Visa Europe and the European Cybercrime Centre at Europol and involved 26 airlines, 38 airports and 16 European countries.

Individuals with airline tickets purchased using stolen payment card details were prevented from boarding flights. This resulted in more than 200 suspicious transactions on the day and 120 arrests as at March 2014, although these numbers continue to rise. Criminals were arrested for fraud, possession of false documents and counterfeit cards, benefit and welfare fraud, people trafficking and immigration offences. Two travellers were arrested on outstanding European arrest warrants.

“Visa Europe is proud to have worked with law enforcement on this Day of Action. Because of great work like this – and our €100 million annual investment in technology – fraudsters face detection and Visa remains a safe and convenient way for customers to pay and be paid,” said Peter Bayley, Executive Director, Risk Management, Visa Europe.

Visa Europe is committed to enhancing both the range and security of payment services to the airline industry. This draws on our heritage in the travel and entertainment sector and our understanding of the special requirements of the airline sector in particular. Building on the success of the airline fraud working meeting and Day of Action, we intend to be involved in - and, where appropriate, lead - further initiatives to combat fraud in the airline sector are planned during 2014.

“Because of great work like this – and our €100 million annual investment in technology – fraudsters face detection and Visa remains a safe and convenient way for customers to pay and be paid”