www.profit.uk.com

PROFiT

Prevention of Fraud in Travel

www.profit.uk.com

INDUSTRY BRIEFING NOTE - UPDATED no. 5

CARD TRANSACTIONS

BACKGROUND

The advance of technology has made it possible to dispense with cash and to transact remotely through a payment card and this method of transacting has become increasingly widespread especially with the move to online and mobile purchases of goods and services.

This industry briefing note identifies a number of practical steps that organisations taking payment cards should adopt to avoid problems such as 'charge backs'.

When all of the correct processes are in place a payment card is a safe, secure, and convenient substitute for a cash transaction.

HOW DO PAYMENT CARDS WORK?

When a payment card is swiped or keyed a transaction for the payment is generated.

Upon approval of the sale, a receipt is given to the customer. For swiped, face-to-face, transactions the customer usually enters their PIN number into a secure encrypted pad, or in a limited number of cases signs a copy of the receipt. In the case of contactless payment pads there is no validation after the card is swiped. Call centre transactions require the seller to enter the card details into their payment terminal. Online transactions require the customer to enter their card details and security code into a template which acts as a substitute for a payment terminal. The transaction takes place once the seller's equipment connects to the payment network and usually only takes 3-4 seconds.

However the payment is initiated the sales information travels from the processing equipment across the secure payment network to where the seller's 'merchant account' is located and an authorisation request is created and sent to the customer's bank where the card was issued. The customer's bank receives the request. If the customer used Chip and PIN then the transaction is already authorised but if Chip and PIN is not used the customer's bank performs a series of tests to make sure there is enough credit available to cover the sales amount.

The authorisation request is either approved, if there are sufficient funds, or declined. A response is sent back to the merchant account, where the transaction is added to a payment batch and then sent back to the originating seller's processing equipment. If the authorisation request is approved, the customer's bank secures funds for the payment.

All transactions go through a settlement process. This process is initiated by the seller closing their open payment batches which are normally processed at the close of business each day. During the settlement process the funds are moved from the customer's bank into the seller's 'merchant account', and then deposited into the seller's business bank account. Depending upon the contract the seller has with the card acquirer it can take varying amounts of time to

settle a payment batch but typically it takes several days. Generally debit card funds are transferred quicker than credit card funds due to the different networks and processes involved.

HOW ARE THE CARD TRANSACTIONS REGULATED?

The Payment Services Regulations 2009 came into force on 1 November 2009 and HM Treasury appointed the Financial Services Authority (FSA) to monitor and enforce them. The FSA has since become the Financial Conduct Authority (FCA).

PROBLEMS WITH CARD PAYMENTS

Either through misuse, theft or personation, a number of payment card transactions will present problems for retailers. Generally merchants face greater difficulties identifying criminal card use when taking remote transactions than they do with face-to-face transactions. A misused, or fraudulently used, card is likely to result in a chargeback to the merchant. Where the card acquirer identified a high number of chargebacks they may pass on a fine to the merchant from the Visa or Mastercard scheme as appropriate.

HOW TO AVOID PROBLEMS WITH CARD PAYMENTS

A wide range of tools are available to combat card fraud. Not all of these tools will be relevant to every business and not every business will find some of the measures cost effective. Many, however, are little more than common sense and can be implemented with a relatively modest investment of cash and, more particularly, staff training.

01 Creating a Risk Matrix of fraudulent transactions

Only certain types of transaction attract a high degree of risk. Every organisation should review card payments where a fraud has occurred and identify the common factors which form a 'risk matrix'. This information should be used to draw up a risk profile for high risk transactions. An organisation may decide to carry out checks on transactions identified using the risk matrix parameters before accepting or declining the transaction.

This is probably the simplest thing an organisation can undertake and if carried out properly it is very effective at reducing the risk of fraud. Because fraudsters do not want great effort in pursuing their aims they tend to use some data repeatedly. The data that reoccurs could be a name, an IP address, postal address, email address or mobile phone number. Whatever the data, when looking at occurred frauds some patterns will be identifiable and these should be brought together to form the 'risk matrix'. On their own each element that occurs when a transaction takes place is suggestive of suspicious behaviour that may warrant investigation; but when multiples of these commonly used factors occur in a transaction then it gives an increasing degree of confidence that the transaction is fraudulent.

The factors that a company should look at to build their risk matrix include:

- Cardholders name,
- The Bank Identification Number,

- The postal address,
- The delivery address (if applicable),
- The domain used,
- The Internet protocol (IP) address used, and
- The phone number used.

Specific industries may have additional factors that reoccur in fraudulent transactions and can be used in the matrix such as passenger names, or the destination, or departure point for the travel industry.

The more information used to build the matrix the more persuasive the matrix will be in indicating a fraudulent transaction. FI Networks specialises in working with the City of London Police, National Fraud Intelligence Bureau (NFIB) to conduct industry case studies in order to identify this type of information and help industry sectors to become more resilient.

As an example of how this can work: Internet technology enables additional information to be recorded which can be analysed at a later date.

Most computers reveal an Internet Protocol (IP) address, which provides information on where the transaction was made. Although this information cannot be relied upon to determine the individual's exact location, it can assist in the post-transaction analysis. If a single IP address shows differing cardholder details it could possibly show a risk of fraudulent activity.

Merchants should be aware that some Internet Service Providers (ISPs) allocate dynamic IP addresses, so the information is not necessarily accurate. If transaction data is available in an electronic form, it can be analysed in an application such as MS Access or MS Excel to help identify fraudulent patterns. This allows merchants to understand the potential risks. This may include identifying addresses where fraud is continually being perpetrated, or perhaps the type of goods that are being obtained.

0.2 High Risk Transactions

02.1 Identification of customers

There has been a large increase in levels of account takeover/identity fraud. As well as the use of fraudulently obtained card details, criminals will use fictitious identity documents in order to obtain goods and services. Identifying such documents is the key to fighting fraud. For further assistance on the identification of fictitious identity documents visit:
http://prado.consilium.europa.eu/en/homeIndex.html.

Unless the customer is already well known to the organisation, where it is practical to do so, try to engage the customer in discussion or correspondence. This may alert you to any suspicious activity.

Be particularly wary of a customer who:

- Uses a payment card that does not match the person making the purchase,
- Shows no regard for the cost of expensive goods or services being requested,
- Demands next day delivery and shows no regard for any additional costs involved,

- Makes a telephone call on the day of delivery asking what time tickets or travel documents are due to be delivered, as it may be a fraudster trying to intercept them,
- Alters the delivery address at short notice.

Fraudsters will try to use a number of methods to arrange delivery to addresses that are not the genuine cardholders'. This could be by way of redirects, mail interception, or collusion with landlords or estate agents. Secure delivery is perhaps the most effective way to prevent such fraud.

Merchants will help to reduce fraud if they:

- Insist that high value items are only delivered to the cardholder's permanent address; if these are to be sent to a different address, merchants should be cautious and obtain detailed proof of delivery.
- Avoid sending high value items such as travel documents to hotels or guest houses; the incidence of fraud involving delivery to such places is extremely high,
- Only send high value items by registered or recorded post or by a reputable security courier, and insist on a signed and dated delivery note.

Couriers should be instructed to:

- Return with the valuable items and travel documents if they are unable to deliver to the agreed address,
- Always deliver travel documents to the specified addressee and be wary of people lingering suspiciously outside the property,
- Obtain a signature from the recipient and ensure the name matches the person ordering the items, documents, or tickets,
- Not deliver papers such as travel documents to a vacant property.

Where suspicions are aroused, it is always a useful practice to ask customers a series of questions to verify their personal details. If they have an existing account with your organisation, ask questions about a previous transaction. Dynamic questioning is a useful approach – using a random set of questions about the details already held on that customer.

Other checks to help reduce the risk of fraud and incurring a chargeback include:

- checking details of new business customers in a local business directory or register,
- obtaining a phone number for the customer's address through directory enquiries and contacting the customer to confirm the order,
- using the 1471 call-back facility – be wary if the phone number has been withheld,
- using a caller display service to ascertain which telephone number a customer is calling from,
- checking order records to see if there are a large number of transactions over a short period of time from a company or person with whom previous business has not been conducted, and
- checking if the delivery address has been used previously with different card details.

PROFiT

Prevention of Fraud in Travel

www.profit.uk.com

INDUSTRY BRIEFING NOTE

With Cardholder Not Present (CNP) transactions, if suspicions are aroused a number of other questions can be asked such as mother's maiden name (even if the answer is not known) to see if the customer answers without undue hesitation.

02.2 Maintaining records of fraud

Maintaining records of fraudulent accounts can be an effective measure to prevent further fraud. As well as repeat attacks from the same offenders (they will always revisit perceived easy targets) the type of offence they commit could be repeated by other fraudsters, so learning from these attacks is vital. If you are able to, load these details into a predictive system it can help to identify suspicious activity.

Alternatively, in smaller businesses, display information on known fraudulent purchases in a prominent place so that all staff are made aware. If such internal hot-lists are maintained, ensure that all transactions are checked against them. If large amounts of fraud occur, post-analysis should be considered. It will allow you to understand where your business is most at risk and how fraud can be prevented in the future. If this analysis is undertaken before the travel date, there is a possibility that early intervention could prevent travel taking place.

02.3 Monitoring accounts

Monitoring the trends of customer registration can be effective in establishing where there are elements of organised criminal activity taking place. Monitor details such as repeated use of delivery addresses and card numbers. If the internet is used, look at the Internet Protocol (IP) address and check if there is repeated use for a number of different and apparently unconnected transactions. You can also check the address on Google Street View to see if it exists.

02.4 First party disputed transactions

Sometimes customers will dispute transactions where they have been a participant but choose to refute any connection. Review existing customer records to identify if the individual has made purchases with your business before. Have they made a similar purchase without dispute in the past? Challenging a customer should be conducted in a manner that is non-accusatory and seeks to establish the facts.

02.5 Staff training

Training staff on the risks of card fraud is a key tool to preventing future losses. Empower them to make intuitive decisions. Insist that questions are asked and that the overall risks involved with such transactions are known and understood. Ensure that regular training updates are given to all staff especially newcomers.

02.6 Risks to smaller organisations

Small organisations can be subject to the highest risk; high value items such as airline tickets have the same value regardless of which operator sells them. Fraudsters are likely to target small merchants in the hope that they will not be as diligent in their verification procedures. Treat each sale with the same approach and obtain confirmation that the cardholder is genuine.

PROFiT

Prevention of Fraud in Travel

www.profit.uk.com

INDUSTRY BRIEFING NOTE

02.7 Out of hours

When automated systems are used, fraud can often occur out of core business hours. Fraudsters will often target call-centres late in the evening or at weekends when staffing levels are lower and supervision or management is often insufficient to allow intervention in suspicious transactions.

Analysing out-of-hours activity before despatching high value items such as travel documents/tickets often proves useful. If at all possible, arrange for I.D. or a credit card to be presented when tickets are to be collected.

Setting credit or transaction limits for out of hours transactions will mitigate the effect of this type of fraud.

Fraudsters often work together and share information on systems they encounter at a travel company. The way fraudsters test systems and then share the information leads to a common pattern of fraud in travel organisations where late on a Friday or during a weekend a number of fraudulent transactions occur one-after- another.

03 Face to Face Transactions

Since the introduction of Chip and PIN, the opportunity to commit card fraud in a face to face environment has reduced considerably, especially in the UK.

That said it is still vital that staff are trained to spot suspicious transactions at the point of sale. Some indicators of fraudulent activity are listed below. Whilst each may have a perfectly innocent motive, the presence of more than one of these may indicate the need for further checks.

- Customers avoiding eye contact, sweating or behaving in an aggressive manner,
- Attempts to distract sales staff during the transaction,
- Customers showing no regard for cost,
- Apparent difficulty remembering PIN numbers,
- Use of a ‘friends’ card,
- Apparent ‘miss-match’ between booking and customer (i.e. first class flights being booked in suspicious circumstances),
- Bookings for long haul destinations with same or next day departures (especially if one way),
- Attempts to use more than one card, especially where one has been declined,
- Requests to split one transaction over more than one card,

Cards should also be examined to see if any of the following are present

- Damaged signature panels
- Blurred printing in the card background
- Card numbers on the front and back of the card not matching
- Miss-match between gender shown on card (not always available) and customer

- Miss-match between 'member since' date shown on card (not always available) and customer. A 20 year old customer, for example, cannot have been a 'member since' 1960!
- Genuine credit cards will fluoresce under a UV lamp (available cheaply off of the internet) in much the same way as banknotes. If suspicions are aroused check that the card presented does so.

04 Code 10 Calls

If a merchant is suspicious about a transaction and wishes to call the authorisation centre, they can alert the operator to their suspicions by telling him/her that he is making a 'Code 10' call.

The operator will also assume that the merchant is unable to speak freely because, for example, the customer is standing next to them.

The call may take a little longer than ordinary authorisation conversations as the merchant will be automatically referred to the fraud prevention department of the issuing bank. Because of the assumed proximity of the card holder, the questions the merchant will be asked will all require a simple 'yes' or 'no' answer.

Code 10 calls should not be made unless there is a genuine suspicion or concern about the transaction, the card or the cardholder. There are multiple reasons to make a Code 10 authorisation request, including:

- After the card is swiped, the point-of-sale (POS) terminal displays a "Lost or Stolen Card," "Pick Up Card" or a similar kind of message.
- During the inspection of the card the merchant discovers that its security features have been altered or tampered with in some way.
- The signature on the transaction receipt does not match the one on the back of the card.
- The customer behaves in a suspicious or unusual manner. You should be careful with jumping to conclusions on this count, as there may be a perfectly legitimate explanation for your customer's behavior.

When making a Code 10 call, make sure that you have your merchant account number and the credit card being used readily to hand.

The authorisation centre will often wish to speak directly to the cardholder. If this happens make sure that you speak to the centre yourself before completing the transaction rather than letting the customer tell what has been said.

There are occasions when the authorisation centre will request you to retain and/or destroy the card being offered or even to delay the transaction whilst the police are called. You should ALWAYS follow your own businesses policy in these cases and NEVER put yourself or anyone else at risk.

If you are unable to make a Code 10 call at the time of the transaction because you feel threatened or concerned about safety, make the call as soon as practicable after the

transaction or when the cardholder has left your premises. This will alert the authorisation centre and may prevent further frauds on that card.

As with all other authorisation calls, a Code 10 call DOES NOT GUARANTEE PAYMENT.

05 PCI-DSS

The plastic card industry has adopted a standard for the handling, processing and storage of credit card transactions which is known as Payment Clearance Industry – Data Storage Standard (PCI-DSS). Everyone that takes payment by payment card is obliged to adhere to this standard which has been introduced to reduce the risk of fraud occurring.
The PCI council oversees the standard and authorisation of key organisations within the system. If you are taking payments face to face or remotely then you must comply with PCI.

To check your organisations compliance please see the PCI Council's website: www.pcisecuritystandards.org.

PCI applies to all cardholder data which is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, etc. All personally identifiable information associated with the cardholder that is stored, processed, or transmitted is also considered cardholder data.

Some key factors required by PCI-DSS include:

- Make sure staff do not note down, or record card numbers,
- Do not store cardholder data unless your systems fully meet the storage, processing and handling criteria for PCI,
- Only transmit card details in a secure and encrypted form,
- If you record calls implement systems to remove or mask the card details when spoken,
- Carry out the self-assessment at the intervals required by PCI,
- Carry out security scans at the intervals required by PCI, and
- Follow the PCI rules and any laws for reporting if your system is compromised.

06 Chargebacks

06.01 Can I dispute a chargeback?

The short answer is 'yes'. Card issuers will investigate claims from cardholders that a transaction is not genuine and merchants are entitled to dispute such claims but should be prepared to support this with documentary evidence. The onus of proof is on the merchant and the final decision will rest with the card issuer.

The merchant is never guaranteed success in challenging a chargeback, but they can increase the chances of success by following some best practice;

- Respond to retrieval requests,
- Respond to 'requests for Information' Chargebacks,
- Use CV2 and AVS,

- Ensure the evidence you provide at 1st chargeback stage is everything you can provide,
- Respond if you have refunded,
- At least one of the passengers/guests should be the named cardholder.

Where the chargeback is due to alleged **fraud** the merchant will need to prove to the card issuer that their cardholder has participated in the transaction and they will want evidence of their customer details matching the genuine cardholder including:

- A copy of the passport,
- Boarding Pass,
- Hotel Registration.

Where the chargeback is alleged to be due to **duplication** the card issuer will want to see evidence of two separate transactions.

Where the chargeback is alleged to be due to the **transaction not recognised** the card issuer will want all the details of the transaction including:

- Date,
- Name of customer,
- Address of customer,
- Card number (truncated is acceptable),
- Amount,
- Date of stay or travel.

Where the chargeback is alleged to be due to **non-receipt of services** the card issuer will need to see proof that the guest has stayed, or that the holiday has been utilised, by the cardholder.

Where the chargeback is alleged to be due to **non-receipt of a refund** the card issuer will want to have the full details of when the refund was processed or details of why a refund is not due to the cardholder.

06.02 Chargebacks & Cardholder Not Present (CNP) transactions

When credit cards were originally introduced, it was never the intention that they were to be used in a CNP environment. Because of this, and because it is inherently more difficult to carry out point of sale security checks in a remote environment all CNP transactions are carried out at the merchants risk. The exception to this is transactions covered by the 3D secure systems (see 07.02).

06.03 Debit Cards

Consumers in the UK who pay for goods and/or services are protected under the s75 of the Consumer Credit Act if those goods and/or services are not supplied or are faulty. The Act gives them the right (subject to certain conditions) to reclaim the cost of goods and/or services from their card issuer. This, in turn, gives rise to the chargeback to the merchant.

It is not commonly known that, under VISA regulations (though not the Consumer Credit Act), the same rights apply to VISA debit cards where the cardholder has bought goods and/or services 'that will not be delivered, for example where a merchant ceases trading, or if the goods are not supplied as specified'. The same right does not exist for Mastercard debit cards

07 Fraud Prevention Tools

07.01 Address Verification and use of the Card Security Code

The UK banking industry introduced the Address Verification Service ('AVS)' and Card Security Code ('CSC') in 2001 to help merchants prevent CNP fraud. AVS and CSC are available to merchants who use the automated electronic authorisation process.

AVS is available for all UK-issued MasterCard, Visa, Maestro and American Express cards. Whilst a fraudster with a lost or stolen card may be able to supply a CSC, it is less likely that they will be able to provide the genuine cardholder's address. The decision to proceed with a transaction is at the merchant's discretion.

AVS checks the numbers in the cardholder's statement address with that held by the card issuer and gives CNP merchants assurance that the customer has provided the correct card billing address. AVS verifies that the billing address of the credit or debit card matches the address that was given by the customer. Because AVS only verifies the numeric portion of the address, certain anomalies like apartment numbers can cause false declines; however, it is reported to be a rare occurrence.

The CSC is a three digit code printed on the back of Visa, MasterCard and Maestro cards, usually in the signature box, and it appears as a four-digit code on the front of American Express cards. The CSC provides CNP merchants with some assurance that the card number provided is a genuine one.

AVS/CSC details are captured electronically by the merchant point-of-sale (POS) system and compared with the details held by the card issuer. CSC can be checked against all cards issued within the EU.

Unlike a PIN or signature, neither AVS nor CSC is a full confirmation of the cardholder's identity. However, when used together they allow merchants to decide whether to proceed with a transaction, so giving a cost-effective fraud prevention tool. Using AVS/CSC to check the cardholder's statement address and card security details is helping many merchants reduce their CNP fraud and chargebacks.

Fraudsters may make a number of attempts to guess the CSC. The likelihood of a fraudster guessing correctly is extremely low. However, if automated systems are used, limit the number of times a user can input a CSC. "Three strikes and you're out" is an effective practical policy to consider.

Storage of customers' CSC data is strictly prohibited under card scheme rules to prevent misuse. This applies to all CNP merchants capturing the CSC electronically, through a voice recognition system or manually. Specific rules for CNP mail order merchants should be obtained from acquirers. Merchants who retain copies of card details or faxes where the CSC may be visible, should blank this information out before storing. Card scheme rules state that merchants undertaking subsequent transactions must not re-use CSC data

AVS/CSC provides an effective fraud prevention tool, but should be used in conjunction with other tools for maximum effect. For internet merchants, the banking industry provides 3D secure Verified by Visa and MasterCard SecureCode, which can give both a confirmation of the cardholder's identity and some protection from chargebacks for certain transactions.

Commercial solutions are also available to help to identify high-risk transactions before an order is processed. Your acquiring bank can discuss the correct combination of these tools for your business.

AVS/CSC is not a full identification of the cardholder, but it does present a significant barrier to the most common CNP frauds. The CSC prevents attacks using the large scale generation of card numbers. It is also effective against more opportunistic attacks where the fraudster has obtained card number details but does not have the actual card in his possession.

Because AVS provides better information relating to the cardholders billing address, merchants can be alerted to situations where a different or incorrect delivery address is provided. Merchants can help themselves to minimise fraud by not delivering to any addresses which have not been checked by AVS. Merchants implementing AVS/CSC have seen reductions in fraud losses of up to 70%.

07.02 3D Secure ("MasterCard SecureCode and Verified by Visa")

Online Authentication services are e-commerce solutions that make cardholders safer from the threat of fraud when they use their cards to shop over the internet. Visa and MasterCard both offer internet authentication solutions, known as Verified by Visa and MasterCard SecureCode. These are international services, and issuers and merchants all over the world are already part of the scheme.

MasterCard SecureCode and Verified by Visa are authentication services that have been developed by the card schemes to provide a more secure approach to credit and debit card transactions over the internet. Cardholders register for the services and choose a private password for use when shopping online at a participating merchant.

Use of these authentication services by a merchant usually shifts the liability from the merchant to the card issuer in the event of a chargeback, under the following conditions:

- Merchant and acquirer have installed the services, but the cardholder is not registered for the service.
- Merchant and cardholder have both registered for the service.
- Merchant and acquirer have installed the services but the issuer is not enabled to operate the service.

PROFiT

Prevention of Fraud in Travel

www.profit.uk.com

INDUSTRY BRIEFING NOTE

- All Verified by Visa transactions globally where the cardholder disputes participation.
- All MasterCard SecureCode transactions globally where the cardholder disputes participation.

To accept Maestro cards over the internet a merchant is required to support MasterCard SecureCode. This will provide protection and support to cards issued both in the UK and globally. As both of the MasterCard and Visa services are based on the 3D Secure protocol, the installation of either service, together with a merchant plug-in, can support both of the card schemes. These services provide customers, merchants and banks with greater security for card payments on the internet. You can register for these services with your merchant acquirer or Payment Service Provider. For more information contact your acquiring bank.

Merchants should be aware that like all counter fraud and verification systems there are limits to their usefulness. In the case of Verified by Visa, for example, a problem exists in the 'forgotten password' protocol. Where a customer forgets their password they are able to change it on line through the 'forgot my password' link where the system will require four pieces of information:

- The Card Security Code (CSC)
- Expiry date,
- Name embossed on the card, and
- Date of birth of cardholder.

The problem is that the first three pieces of information are all printed on the card itself and so will be in the hands of anyone that has stolen the card, or has the details as they are posted on a 'sucker site'. Dates of birth are also widely available as it is widely shared on social networks, surveys, sign-up forms and a myriad of other places and also freely available in public records online.

Having entered the required information all that remains is to enter a new password of your choosing and your transaction is authorised. Worse still, no email notification is sent to alert the cardholder that their account has been accessed or modified. The cardholder need never know that their card has been compromised until they check their statements. This allows a fraudster, who can obtain this data, to change the password and misuse the card to commit fraud with a low risk of capture.

In 2014 Mastercard and Visa announced that they are removing the need for users to enter their passwords for identity confirmation as part of a revamp of the existing 3-D Secure scheme. The arrival of 3D Secure 2.0 during 2015 sees the credit card giants moving away from the existing system of secondary static passwords to authorise online purchases, as applied by Verified by Visa and MasterCard SecureCode, towards a next-generation system based on more secure biometric and token-based prompts.

PROFiT

Prevention of Fraud in Travel

www.profit.uk.com

INDUSTRY BRIEFING NOTE

08 Third Party Solutions

Merchants should be aware that, as well as the best practices and industry solutions recommended, there are a number of suppliers in the market offering solutions designed to assist in combating fraud. Your merchant acquirer may be able to provide further details of these and other systems. You should always check which solution is appropriate for your own needs.

08.01 Industry Hot Card File ('IHCF')

The Industry Hot Card File is a computerised list of reported lost and stolen cards available to merchants to assist in the identification and prevention of fraudulent transactions. The IHCF enables retailers to electronically check every card transaction for cards being used fraudulently.

More than 60,000 retailers subscribe to this electronic file that distributes data on lost or stolen cards. The IHCF is now also used by over 850 merchants operating in the Card-not-Present (CNP) environment (for example, those businesses which handle telephone orders or trade online).

When a card is swiped as part of a normal transaction it is automatically checked against the file. If the details given match those of a card on file an alert is given to the retailer. The file is provided to merchants by one of the Accredited Data Recipients (ADRs):

- **Fidelity Information Systems** www.fismerchantpayments.com

Merchants who are interested in receiving the IHCF should approach the ADRs who will be able to assist with any enquiries and take forward requests.

Mastercard and Visa also will issue lists of their own stolen and compromised cards which merchants can obtain via their card acquirer. Bank issued compromised card lists and IHCF are, by their nature, historic and there is generally a delay between when a card is misused and when it appears on a list in circulation. For travel companies this delay will often allow the fraudster to act and travel before the merchant is made aware of the issue.

08.02 Identity and Transaction Checking Systems

Identity checking systems verify data provided by the customer against databases held. This enables the system to indicate the likelihood of the data being correct. Whilst each system essentially does the same thing, there are variations in the way in which the vetting is done, the databases used, the information needed and the way in which each search is reported back.

There are basically three methods used in identity or transaction verifications systems which can be classified as:

- **Broad data systems** which access data from a number of different sources and check limited details against them,
- **Deep data systems** which access one or two sources of data only but which generally look at a wider spectrum of details and check against them, and
- **Database systems** which work by storing details which might indicate a problem and check the identity or transaction against it.

There is only one system on the market known to be using live data at the present time with virtually all other systems using cached data which may be of indeterminate vintage.

Users generally find that where they employ more than one of the currently available tools they are less than 100% effective and where two or more systems are used concurrently they may act against each other.

09 Data sharing

Merchants who are able to, share information with other merchants that have been targeted by CNP fraud in order to reduce the risks. This is effective where enough merchants are in the group, but all merchants should be mindful of the Data Protection implications of this type of activity and we would urge that full advice is sought on how to comply with the law before this is undertaken.

10 THE FIN TOOL

The FIN tool is the first of a new generation of counter fraud products which does not work by verifying data against third party information, but instead applies powerful analytics to determine whether suspicious activity or fraud is occurring. The system operates in rteal time and features alerts and the opportunity to find out more information when it spots suspicious activity occurring.

11 Banking Issues

11.01 Phishing Emails

There has been an explosion of convincing looking emails purporting to be from a bank or card scheme alerting companies and card holders to the fact that their accounts have been compromised and that the solution is to use a link in the email to change passwords. These emails are not genuine and are used by fraudsters to take over computers, load malware onto computer systems, embed spyware into IT infrastructures and steal money from bank accounts. This type of activity is known as a phishing attack.

Genuine banks and card schemes *never* send alerts such as this by email and would never ask you to use an embedded link, or phone someone, in order to change password. If possible, configure your systems to filter out this type of phishing attack or quarantine them.

Where it is not possible to intercept them, make sure staff are regularly reminded not to open these emails and that they should delete them immediately. If you do suffer such an attack seek the help of an IT professional immediately.

11.02 Bank Account Takeover

Several companies have experienced their bank accounts being taken over by fraudsters. One way this can happen is through a bank's use of activation codes. Some banks use activation codes to enable a bank account to be used. These are generally sent by text to a mobile phone. Where a criminal is able to get hold of the mobile phone registered to the bank, or alternatively, to persuade the bank to change the receiving mobile phone, they are able to

access the bank account. Criminals persuade phone providers to divert mobile phone numbers in what is sometimes called "SIM swap fraud". Some banks text security details when customers forget their details. The activation codes sent by text to mobile phones also allow payments to be made from an account.

The scam works by blocking the genuine phone. The owner is unaware of why the phone has been blocked and allows the criminal - who now has control of their phone - to syphon money from their bank account. http://www.bbc.co.uk/news/business-35716872

Companies should be alert to this type of activity and should anything unusual occur with the bank account or key mobile phones, investigate and take appropriate action to protect funds.

11.03 Payment Request Fraud

Every year hundreds of companies are caught out by payment request frauds. Although these masquerade as different things they are, in fact, all variations of the same thing: making your finance team pay a debt which is not owed.

For many years we have become used to receiving requests for payment through the post falsely alleging that payment is required to maintain a trademark, European trade mark, directory or registry entry, or similar. These are usually sent out around periods when staff holidays are more likely and rely on the finance team paying without making proper enquiries, even though no invoice is in the system.

More recently we have become used to emailed payment requests regarding domain use in overseas, notably Chinese, registries. To overcome all of these frauds is easy, namely only pay out when an order is in the system, and where one does not exist check with the person that normally deals with such matters.

The most recent incarnation of payment request fraud is known as ‘CEO Fraud’ to police and involves an email to the finance team purporting to come from a very senior member of the management team such as the CEO, Sales Director, Owner, MD, Marketing Director or similar. The email states that they need something paying immediately. In fact the email is not genuine and is a spoof of the person named.

The scam relies upon the finance team responding to the email to enquire about the bank details of the recipient. Of course, the finance team are actually responding to the fraudsters who direct them to their own bank account and not the person they believe sent the email. Once paid it is very difficult to recover any of the lost funds.

This type of fraud is easy to overcome. Initiating a simple rule whereby any request for payment that is not supported by a pre-existing invoice is not paid until the actual named person has been spoken to will stop this fraud directly. When speaking to the named person it is important to do so either in person in the office, or on their mobile number, if they are out of the office, and get them to, ideally raise an order, or at least confirm that the payment is to be made.

NOT A PROFiT MEMBER?

PROFiT works on behalf of the whole industry to spread best practice and combat crime. We can only continue do this with industry good will and support so why not join us and help fight travel crime and reduce the risks for travellers and travel companies. Contactus@profit.uk.com.

PROFiT

Prevention of Fraud in Travel
www.profit.uk.com
INDUSTRY BRIEFING NOTE

HOW TO AVOID PROBLEMS WITH PAYMENT CARDS

The following tips on how to minimise the risks.

1. Analyse your fraud transactions to draw up a high risk matrix of the common factors and use this to identify transactions that should not be processed, or that you choose to make further enquiries about, before processing.
2. Make sure you and your organisation are fully Payment Clearance Industry Data Storage Standard compliant.
3. Train your staff to recognise and deal with fraud.
4. Use third party counter fraud tools.
5. Implement 3D secure for your systems.
6. Consider Address Verification Service (AVS) and Card Security Code (CSC)
7. Maintain records of fraud.
8. Monitor accounts.
9. Share data with other merchants.
10. Consider using the industry Hot Card File.
11. Consider the FIN tool as a method of sharing data and identifying fraud attacks.
12. If you become a victim of fraud e-mail 'action fraud' www.actionfraud.org.uk with the details and keep all of the evidence.

1st draft released December 2013