



# VISA FIGHTS FRAUD

## PAYMENT CARD FRAUD

September 2004

### What is the current Fraud Experience?

Through its 21,000 Member banks, Visa offers cardholders around the world with the opportunity to shop in over 20 million “bricks and mortar” merchants with an additional vast range of e-commerce merchants. The merchants, so long as they follow basic Visa rules with regard to technology and acceptance will usually receive a guarantee of payment and the cardholder can leave with their goods and services almost immediately.

Within Europe alone, Visa cardholders undertook over 12.3 billion transactions during 2003, representing expenditure volume of over €824 billion and it is an inevitability that Visa cards and transactions, in the same way as any other financial payment system, are occasionally targeted for fraud.

However, fraud losses currently accounts for less than €0.00065 for every Euro spent via the Visa system, and this level has been decreasing for over three years.

Visa Members remain committed to reducing fraud losses to the lowest possible level and as such fraud loss levels, together with the circumstances of loss, are monitored closely so as to ensure that appropriate actions can be taken to address payment card fraud

Examples of fraud definitions within Visa are:

- Card Not Received – fraud loss suffered on cards intercepted between manufacture/personalisation by the card issuer and delivery to the customer
- Lost / Stolen – losses incurred on cards either lost or stolen from the genuine cardholder
- Counterfeit – fraud undertaken using fraudulently manufactured cards at physical merchants.
- Card Not Present (CNP) – losses occurred as a result of card numbers being used to undertaken transactions within the electronic commerce, mail order or telephone (“MOTO”) order environments

## Visa's Solutions:

Visa has developed a range of tools and services to allow fraud loss to be managed effectively. These include:

### Chip & PIN

A major infrastructure implementation which fundamentally strengthens the overall payment security and will allow better management of Card Not Received, Lost/Stolen and Counterfeit Fraud losses.

### Verified by Visa (VbV)

A major infrastructure build which fundamentally strengthens overall payment security and will allow better management of e-commerce transactions

### Visa's Intelligent Scoring of Risk (VISOR)

Visa's fraud detection solution which uses neural network technology to assess how each genuine cardholder uses their card, compared to that of known fraudulent activity. This allows issuers to identify fraud (of all types) and thereby minimize losses and reduce cardholder inconvenience where fraud occurs.

### Account Information Security (AIS) Programme

The AIS program is designed to protect sensitive account and transaction information in the Visa acceptance environment. It protects the interests of all payment participants, including Members, merchants and cardholders—in both the physical and virtual world. Visa was the first in the industry to create such a program, including standards, best practices and self-assessment security tools. The AIS program also created a Global Data Security web site for merchants to assess their vulnerability to Internet hacking using a free and confidential online tool and also gives them access to Visa's best practices and standards. The website address is [www.visa.com/secured](http://www.visa.com/secured)

## Cardholder Messages:

Visa has a wide range of initiatives in place to tackle payment card fraud  
The levels of payment card fraud are dropping rapidly with the Visa Europe region

### **Bricks and Mortar Shopping**

Report any loss of your cards immediately to your card issuer

When you receive a new or replacement card, memorise the PIN number and destroy the paper it is written on

Never divulge your PIN number to anyone. If you are concerned that someone may have got hold of it, contact your card issuer immediately

Take a note of the account numbers of your cards, together with the emergency contact numbers of your card issuers and keep these separate from your cards, whether at home or abroad. Alternatively you may call the Visa 24 hour emergency number corresponding to the country you are calling from. You will find a list on [www.visaeurope.com](http://www.visaeurope.com)

Keep an eye on your card when you hand it over to be swiped at a shop or in a restaurant and always check that the information on the sales voucher is correct before signing. Ensure your card is handed back to you

If you are at a cash machine and someone behind you is behaving suspiciously or attempts to distract you in anyway, move to another machine. It is possible that they may be trying to discover your PIN for fraudulent later use.

Never drop or leave behind your receipts when using a cash machine or purchasing goods/services– these may well have your card details on them. Keep them until you have checked them against your statement and then dispose of them safely

Always check your statement to ensure that you can account for every transaction. Contact your card issuer if there are any transactions you believe you didn't make

## Shopping on the Internet

If you're not familiar with an online shop, check their statement regarding security on the site (terms and conditions and privacy policy) or call their customer help line number to reassure yourself before making a purchase.

Make sure you can return any unsatisfactory items and check to see if your money can be refunded or if you will receive a 'credit note'. Read their privacy policy and also their sales policies that should cover the delivery methods, cost of delivery, currency accepted, taxes applied, return and refund policy, and a contact number or mailing address – in addition to the e-mail address. Be aware that purchases from private sellers may be more at risk than those from registered businesses.

When making online purchases, ensure you are using a computer that has appropriate levels of security e.g. anti-virus software and a firewall.

Keep your software up-to-date. Download from the relevant entities and apply patches regularly to ensure operating system, main applications, virus checkers and firewalls are all performing as well as possible.

Keep your passwords private and try to change them often. Create passwords that are difficult to figure out (avoid obvious passwords like your name, your birth date or your telephone number). Create passwords that use a mix of letters and numbers.

Keep a record of your transactions - Just as you would save your receipt in the real world, keep a record of all online transactions, including the merchant's contact details and URL (Internet address)

Shopping confidently online – Visa has introduced “Verified by Visa”, a new service to give Visa cardholders complete confidence when shopping on the Internet. Further information on the service and how to join is described on [www.visaeurope.com](http://www.visaeurope.com)

Beware of unauthorized e-mails or sites fraudulently requesting information such as bank card PINs – do not divulge such information unless you have been given explicit instructions by your bank that such use is appropriate. Do not accept these instructions via the Internet (e-mails, etc.), as they themselves may be fraudulent.

When asked to provide payment details, ensure you are at the correct site. Check URL and also for presence of padlock. Clicking on the padlock reveals more information regarding owner of the certificate. If not sure, contact site owner and find out what you should look for with respect to these details.