ONLINE FRAUD PREVENTION

GENERAL ADVICE

The following advice will help minimise your chances of becoming a victim of payment card fraud.

- Guard your cards and card details.
- Don’t let your card out of sight when making a transaction.
- Ask the retailer to confirm the amount being debited from your card.
- Carefully discard your card transaction receipts. Shred all your receipts and documents that contain information related to your financial affairs.
- Check your receipts against your (online) statements carefully. If you find an unfamiliar transaction contact your bank immediately.
- Never write down your PIN and never disclose it to anyone, even if they claim to be from your bank, card issuing company or the police.
- Don't keep your chequebook with your cards.
- Sign new cards as soon as they arrive.
- Cut expired cards into several pieces including through the magnetic stripe and/or chip when replacement cards have arrived. Dispose of the pieces in different locations (e.g. different bin bags).
- Don't leave your cards unattended in a bag, briefcase or jacket pocket in a public place and keep your personal belongings with you at all times.
- When making online transactions, make sure you are using updated antivirus and operating system software.
- Exposure of your card data can be avoided by using systems like PayPal, iDeal and online banking to pay for goods and services.

LvM 09072010 v7.1

TIPS AND ADVICE

to prevent payment card fraud happening to you

EUROPOL

INTRODUCTION

With many people becoming a victim of payment card fraud every year, Europol recognises the need to inform all European consumers about basic fraud prevention methods when using a payment card, whether it is a debit, credit, prepaid or any other value card.

This leaflet is designed to help prevent payment card fraud happening to anyone who uses one or more payment cards, especially during the holiday season, when you and people around you may be using their cards in countries and places they are unfamiliar with and are therefore more vulnerable to fraud.

On 1 January 2010 Europol acquired a stronger mandate and new capabilities to fight serious international crime and terrorism. Under a reform of its legal framework, which establishes Europol as a formal EU agency for the first time in its history, Europol now benefits from increased powers to collect criminal information and a wider field of competence in supporting investigations of serious offences.

Europol provides, amongst all serious and organised crime areas, training and awareness sessions to law enforcement and judicial authorities and other relevant parties inside and outside the EU, on everything related to payment card fraud, counterfeiting of payment cards, trends and how to combat this type of crime in cooperation with all available partners.

Training materials such as sample cards, skimming devices, movies and examination devices support the presentations, and participants are actively involved in the training sessions. The modules are designed and kept up-to-date specifically to be useful and interesting to all levels of investigators and related partners in this type of crime. For more information, please contact Europol directly or, if applicable, through your Europol National Unit.

ATM FRAUD PREVENTION

The basics that everyone should know:

Cash machine (ATM) fraud is not a *type* of fraud, but describes the location where it occurs. ATMs are normally a very safe way of withdrawing cash and accessing banking services, although, unfortunately, they do attract criminal attention.

The following advice will help to minimise the chance of becoming a victim of such crime.

- Be aware of others around you. If someone is behaving suspiciously or makes you feel uncomfortable choose a different ATM. Don't be distracted by other people during your transaction.
- If you spot anything unusual about the ATM, or there are signs of tampering, do not use the machine and report it to the bank or police immediately.
- Be alert. If someone is crowding or watching you, cancel the transaction and go to another machine.

- Stand close to the ATM. Always shield the keypad with your spare hand and your body to avoid anyone seeing you enter your PIN.
- When entering your PIN pretend to push other keys as well to make it more difficult for bystanders (or installed cameras) to recognise your genuine entered PIN.
- If the ATM does not return your card, report its loss immediately to your bank.

Point of Sale FRAUD PREVENTION

The basics that everyone should know:

Skimming can occur at retail outlets - particularly bars, restaurants and petrol stations - where an employee can put your card through a device (without your knowledge) that electronically copies data from your card's magnetic stripe. This information is then usually sold on higher up the criminal ladder where counterfeit cards or clones of your card are made.

Often you will be unaware of such fraud until your statement shows transactions you never made.

The following advice will help minimise the chances of becoming a victim of such crime.

- Be alert and aware of others around you. Don't be distracted by other people during your transaction. If someone is crowding or watching you, cancel the transaction.
- If you spot anything unusual about the payment terminal, or there are signs of tampering, do not use the terminal and report it to the shop owner or police immediately.
- Stand close to the terminal. Always shield the keypad with your spare hand and your body to avoid anyone seeing you enter your PIN.
- When entering your PIN pretend to push other keys as well to make it more difficult for bystanders (or installed cameras) to recognise your genuine entered PIN.

- Never lose sight of, and don't hand over, your card during payment transactions whenever and wherever possible. Insist on having your card visible to you at all times.