BE SMART WITH YOUR CARD

TIPS AND ADVICE TO PREVENT PAYMENT CARD FRAUD HAPPENING TO YOU

GENERAL ADVICE

The following advice will help minimise the chances of becoming a victim of payment card fraud:

- Keep your cards and card details safe.
- Don't let your card out of sight when making a transaction.
- Carefully discard your receipts from card transactions.
- 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 police.
- Your bank will never call to ask for your credit card number or PIN.
- Don't keep your chequebook with your cards.
- Sign new cards as soon as they arrive.
- Cut expired cards into several pieces including the magnetic strip and/or chip when replacement cards arrive. Dispose of the pieces in different locations (i.e. 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.
- Make sure the website you are using for online banking or making payments is secure and encrypted. Use websites beginning with HTTPS and SSL (Secure Sockets Layer) for your online transactions.

PREVENTION

The basics everyone should know:

Card skimming can occur at cash machines (**ATMs**) and retail outlets (Point of Sale (**POS**) terminals).

Skimming occurs when an illegal device is fitted to an ATM, or retail staff put your card through a device without your knowledge, and the data from your card's magnetic strip is electronically copied. The data is usually then sold on higher up the criminal chain where counterfeit or clones of your cards are made. You will often be unaware of such fraud until your statement shows transactions you never made.

The following advice will help minimise your chances of becoming a victim of such crimes:

- Be alert and aware of others around you. If someone is behaving suspiciously, crowding or watching you, choose a different ATM, POS or cancel the transaction. Don't be distracted by people you don't know during your transaction.
- If you spot anything unusual about the ATM or POS, or if there are signs of tampering, do not use the machine and report it to the bank, shop manager or police immediately.
- Stand close to the ATM or POS. 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 real PIN.
- If an ATM does not dispense money or return your card, report this immediately to your bank.
- Use different payment cards for the door opener at banks and the ATM inside.
- Never lose sight (and, if possible, touch) of your card during payment transactions. Insist on having your card visible to you at all times.

PO BOX 90850; 2509 LW THE HAGUE; THE NETHERLANDS; PHONE: +31 70 302 5000; E-MAIL: FOMU@EUROPOL.EUROPA.EU