Payment Card Fraud Prevention Alert

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

This information leaflet is intended to prevent payment card fraud from happening to any cardholder, especially during the holiday seasons when people are likely to use their cards in places they are not always familiar with and are therefore more vulnerable to fraud by default.

The following advice will decrease the chances of becoming a victim of payment card fraud.

This Europol Alert serves the purpose of highlighting general prevention and awareness in the use of all kinds of payment cards in offline and online environments.

General advice

•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 receipts from card transactions. Shred all your receipts and documents that contain information related to your financial affairs.

•Check your receipts carefully against your (online) statements. 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.

•Don't keep your chequebook with your cards.

•Sign new cards as soon as they arrive.

•When replacement cards arrive, cut expired/unused/blocked cards into several pieces, including through the magnetic strip and/or chip. Dispose of the pieces in different locations (i.e. different bin bags or some pieces at home, others at work).

•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.

•Exposing your card data can be avoided by using systems like PayPal, iDeal, prepaid cards and online banking to pay for goods and services.

Cash machines (ATMs)

•Be aware of others around you. If someone is watching you, behaving suspiciously or making you feel uncomfortable, choose a different ATM. Don't be distracted by people you don't know during your transaction.

•If you spot anything unusual about the ATM, such as loose parts (keyboard, screen, card entry slot), or there are signs of tampering, do not use the machine and report it to the bank or police immediately.

•Stand close to the ATM. Always shield the keypad with your spare hand and your body to avoid anyone seeing you enter your PIN.

•If the ATM does not return your card, report its loss immediately to your bank.

Payment Terminals (POS)

Skimming can occur at retail outlets; particularly bars, restaurants, parking ticket machines and (unmanned) petrol stations.

•Never lose sight (and, if possible, touch) of your card during payment transactions.

•Insist that your card is visible to you at all times.

Travel (Hotels, bars, restaurants)

If you are staying in a hotel, it is regular practice to ask for your credit card to secure payment of the room (and facilities). The card number and your name should be sufficient for them. However, often more details are requested as standard procedure:

•Do **not** allow the merchant to make a photocopy of the reverse side of the card (the front only is okay and sufficient). This avoids fraud with the 3-digit code on the reverse side. If this happens anyway, and you cannot prevent this action from being reversed, consider blocking the card immediately.

•If the merchant swipes the card to validate it, ask what is done with the data, which data is stored, how, where, and for how long. If it is stored locally in a text file, it should be considered a risk and you might want to consider blocking the card. If stored encrypted or remotely (e.g. at headquarters), there is a lower risk of your data being stolen or misused.

•Do not provide the PIN of the card (if you have one) **beforehand** unless paying the final bill. This prevents potential full access to the card's balance.

•Make sure that you get your card returned to you and that it is not kept as a 'deposit'. Although bars, cafés, clubs and restaurants are doing this more and more, when opening a tab or ordering a meal, it is not safe. As an alternative, you could provide them with a secondary (debit) or dummy card.

•Do not hand over ID documents (e.g. passport, driver's license) as a 'deposit'. Photocopies are fine, but it should be either/or - either your ID or credit card details. Giving both enhances the risk of fraud or even ID theft. Ultimately ask for the photocopies to be destroyed, or handed over to you, upon leaving.

•Although rare, some hotels store personal data (including credit card details) on their electronic key cards. Since you can never be entirely sure what is stored on these cards, make sure you keep the card with you at all times during your stay and either keep the card after your stay and destroy it (as described above) or ensure yourself that the electronic data is properly erased/wiped/overwritten. Never dispose of used key cards in public bins.

In principle in most cases you are protected against misuse of your payment card and its balance, however it can still cause a lot of inconvenience when a card is blocked and needs replacing. **So prevention is better than cure!**

What to do in the unfortunate case that you become the victim of payment card fraud or ID theft?

•Immediately contact your issuing bank or company to cancel the affected card(s) and freeze the associated account(s) immediately.

•If possible try to transfer all the money out of the affected account.

•If possible try to avoid depositing large amounts of money (e.g. wages) into the affected account(s).

•Report the crime to the local police.

•Keep an eye on your (online) statements and report suspicious money transfers to your bank. In principle the damage will be reimbursed, but sometimes only after an internal investigation is finalised. If you are facing costs (own risk) or damages we can advise how you can prevent being charged for this.

•If the damages are initially large, you might want to consider a temporary alert on your credit through companies like Experian (contact the issuer for more information) to avoid difficulties when trying to apply for loans, credit, insurance, mortgage, investments, mobile phone subscriptions, licenses, etc.

•Keep an eye on your credit reports to ensure no-one has opened any new accounts in your name.