TYPES OF FRAUD AND PROTECTION METHODS

To learn how fraud is committed, how to protect yourself from fraud, and what actions you should take, carefully read the information below.

Types of Fraud

Advance Fee Fraud

Fraudsters advertise non-existent or non-owned products and services on the internet/social media by placing ads imitating the websites of well-known brands or creating different websites.

- ✓ Verify the trustworthiness of the website, person, or institution you are purchasing from. Ensure that the internet site where you are shopping has a valid and up-to-date SSL certificate.
- ✓ Do not accept delivery of a product without checking it when making purchases through social media and the internet.
- ✓ When transferring money for hotel or vacation reservation campaigns seen on social media, you should be cautious. The person or persons you send money to may be scammers. Using reliable websites and companies for hotel and vacation reservations is crucial for your transaction security.
- ✓ When conducting transactions through a notary, ensure that the notary procedures are completed before the money transfer, and verify if the person or institution you are dealing with is genuine.

Fraud through Social Engineering Methods

In this type of fraud, scammers pose as public officials (police, prosecutor, banker, etc.) or attempt to persuade you through various promises (campaigns, chip points, fee refunds, job placement, overseas travel, etc.) to obtain your personal information or make you perform desired transactions.

- ✓ Scammers may identify themselves as public officials (police, prosecutor, judge, etc.) and try to scare you by claiming your association with a terrorist organization or the use of your bank account by a terrorist organization. They may try to convince you to make a money transfer, obtain your card information (including entering the card PIN), or disclose your identity.
- ✓ They may claim there is a problem with your bank accounts/credit cards or promise a refund.
- ✓ They can be very convincing and offer irresistible opportunities.
- ✓ They may claim the offer is only valid for you.
- ✓ To gain your trust, they may provide your credit card number or examples of your banking transactions.
- ✓ They may keep you on the phone for a long time to distract you.
- ✓ Scammers may contact you, claiming you can win large sums of money on illegal gambling/betting sites. They might even send you some money to gain your trust and later request its return. Do not send money or share your information with individuals making such requests.

- ✓ Do not send money or share personal information or card details with strangers making promises of marriage, job placement, overseas travel, earning money, etc., through dating sites or social media.
- ✓ Scammers may contact you using numbers similar to well-known or familiar call center numbers. They may introduce themselves as public or bank employees, request your private information, or ask you to click on a link received via SMS.
- ✓ Do not trust individuals who contact you by phone, SMS, or social media channels, promising gains or discounts with statements like "Send us money with a reference number, then double it back or get a discount." Do not send money and do not share personal or card information.

If you encounter such situations, do not trust the callers and end the conversation immediately.

Fraud through Malicious Software

Various websites, smartphone application markets, and SMS notifications may publish applications, files, or links that seem harmless but can provide access to individuals' devices.

To avoid falling victim to such fraud:

- ✓ Always keep your device software and security applications up to date.
- ✓ Obtain a reliable anti-malware application.
- ✓ Ensure the source of the sent content is trustworthy.
- ✓ Do not download files, games, applications, etc., from any source you do not trust, and do not click on any links.

Phishing Attack Method

In phishing attacks, fraudsters reach out to you through different sources (SMS, email, social media messages, etc.) to convince you to provide your personal or card/account information. The message or notification sent may mimic a known or secure email address.

- ✓ You may be asked to click on a link in the notifications or respond to the notification.
- ✓ In such a situation, never click on the link and do not enter personal information/passwords on unfamiliar links.
- ✓ Be cautious with notifications from unknown sources and do not share your personal information.

Fraud through Lost or Stolen Cards

In such frauds, transactions can be carried out with lost or stolen cards, and information about cardholders can be used without their knowledge.

- ✓ Remember that you are responsible for ensuring the security of your cards and passwords.
- ✓ If you suspect the security of your cards or passwords, immediately inform your bank and United Payment.
- ✓ Cardholders are liable for damages arising from unauthorized use of their cards within the twenty-four hours preceding the loss or theft notification, limited to up to 250 TL. The amount

related to the damage caused by the faulty and unauthorized transaction cannot be offset against the relevant amount unless it is determined and proven.

EASY PRECAUTIONS YOU CAN TAKE

Protect Your Password

- ✓ Do not share or enter your authentication credentials (username, password, one-time password sent via SMS to your mobile phone, passphrase, card PIN, etc.) with anyone.
- ✓ Remember, government agencies, law enforcement, prosecution, police, and financial institutions will never ask you to enter or disclose your password in any way.
- ✓ Do not seek assistance from third parties while conducting transactions at ATMs, kiosks, or smart safes.
- ✓ If your card is retained by the ATM or kiosk, please contact our customer service immediately.
- ✓ If you detect any unusual situation, device, or apparatus at ATMs, kiosks, or smart safes, please inform the owner/operator of the ATM/kiosk.

When setting a password, adhere to password security standards:

- ✓ Choose a combination that does not contain consecutive numbers.
- ✓ Opt for a combination that does not evoke your or your close ones' birthdates and is not the founding year of your favorite team.
- ✓ A combination that does not include national days and holiday dates will keep you secure.

Keep Your Computer and Phone Updated

- ✓ Regularly update the system of your devices and do not download applications from environments other than the application market (Google Play, App Store, Windows Store, etc.).
- ✓ Before downloading applications from application markets, thoroughly research products that approved and well-known developers do not produce.
- ✓ Acquire malware protection software to safeguard your devices.
- ✓ Do not open email and SMS messages sent to you without your permission.
- ✓ Never consider emails or SMS messages that resemble United Payment and request you to update your information or claim you have won a prize.
- ✓ United Payment never calls its customers to request any personal information for any reason.

The responsibility for the protection of your personal information, and card/account password information rests with you. Check your user agreement to learn about your other responsibilities.

IN CASE OF ANY SUSPICIOUS TRANSACTION OR FRAUD, IMMEDIATELY CONTACT UNITED PAYMENT CUSTOMER SERVICE AT 0850 252 22 22.