SECURITY INFORMATION

WHAT IS SECURITY INFORMATION?

Your security information means any type of your:

- client number;
- password;
- authentication numeric code delivered via SMS to your mobile phone;
- or any other access method that PAYMONT gives you as a secure access to your payment account.

HOW TO KEEP YOUR FINANCIAL INFORMATION SAFE

- Dispose of information relating to your account details and security information in a secure manner and never in a public place;
- Don't leave any device registered with your security information unattended;
- Regularly change your password to your PAYMONT Internet Banking application – at least once per 12 months;
- Regularly monitor your account balance. You can easily do this via PAYMONT Internet banking, regularly sent statements set up as per your requirements or through PAYMONT support line;
- Check your statement and compare your transaction receipts;
- Don't respond to unsolicited emails, telephone calls or text messages requesting your account details or your security information, even if the email, telephone call or text message appears to come from PAYMONT. PAYMONT will never ask you to disclose any of your details or security information in this way;
- Read correspondence from PAYMONT before discarding it as it may contain important payment account information;
- Notify us immediately of any changes to your address or other contact details;
- Secure and regularly check and clear your mailbox to help prevent mail being stolen.

WHAT TO DO IF YOU NEED HELP

You need to let us know immediately if:

- Your device registered with your account, your account details or your security information may be lost, stolen or you think someone else may know them;
- There has been an error, unauthorized access, unauthorized transaction on your payment account or if you need to dispute a transaction.

Please notify us immediately on:

- + 370 627 51 117
- +420 296 187 878
- support@paymont.eu

THINGS YOU CAN DO TO HELP PROTECT YOURSELF

Your PAYMONT security information are key to your payment account(s) with us, so you must take special care to safeguard them. Unfortunately, the theft, fraud and loss might occur, but there are steps you can take to minimize your risk. These steps are of informative and guideline character only.

They contain information about how you can maintain the security of your security information to avoid losses. Liability for unauthorized electronic transactions on payment accounts will be determined in accordance with the General Payment Services Agreement and not by the information in this leaflet.

PROTECT YOUR SECURITY INFORMATION

- Remember your Security information;
- Don't tell anyone your security information (mainly password), including family, friends, merchants, Police or PAYMONT staff. Under no circumstances should PAYMONT staff ever ask for your password;
- Make sure no one watches when you enter your password when logging into PAYMONT Internet Banking application. Always be careful to shield your password when using PAYMONT Internet Banking application. Use your free hand to cover the keyboard while you enter your client number or password for PAYMONT Internet Banking application;
- If you record your security information to help you remember them, they must be reasonably disguised so they cannot be easily deciphered;
- Avoid using PAYMONT Internet Banking through free wi-fi at places which record dialed numbers such as hotels, cafes, shopping malls, etc.;
- Do not create your password in a sequence that can be easily guessed, including reversing the order of your client number, disguising it as a number or replacing the numbers with letters;
- Do not record your client number and/or password (disguised or otherwise) on your phone, in your computer or on PAYMONT documents (e.g. agreement, account statements, etc.);
- Do not disclose your client number and/or password in an e-mail, SMS or on social media networks;
- Do not select something obvious when you create your password. Examples to avoid are: your birthday, middle name, family name, driver's licence number, your previous code, reversing the numbers, your postcode, consecutive numbers, phone numbers or numbers which form a pattern.

TIPS TO PROTECT YOUR SECURITY INFORMATION WHEN USING PAYMONT INTERNET BANKING

- Make sure no one watches you enter your security information when using PAYMONT Internet Banking;
- Never access PAYMONT Internet Banking site via an unsolicited email link. PAYMONT will never send an unsolicited email with a link to Internet Banking;
- Do not allow your device to save any of your Security information, including in your browser or password manager;
- Maintain up to date virus protection and firewall technology on your computer and mobile device;

- Remember to log off when finished with your Internet Banking session or if you walk away from your computer;
- Don't share or record your Internet Banking App information within emails or social media accounts e.g. Facebook or Gmail;
- Only use PAYMONT Internet Banking in a safe and trusted environment. Be cautious when using computers in public places such as Internet cafes, hotels & airport lounges.

USING INTERNET BANKING ON A MOBILE DEVICE

- Be careful about what applications you install on your mobile device. Only install applications from official sources such as the Apple App Store or Google Play etc.;
- Ensure that you apply the latest updates as they become available for your device;
- We recommend that you setup a Mobile Device Passcode for your mobile device that is required when you switch it on;
- Your Mobile Device Passcode must be different to any other Secret Code(s);
- Don't store and save personal information such as account numbers and security information on your mobile device;
- If you lose your mobile device, we recommend you change your Internet Banking password immediately (or call us to block your Internet Banking user account).

USING SOCIAL MEDIA AND PROTECTING YOUR IDENTITY ONLINE

- Keep your personal details private. Don't divulge personal and geographic information when using social media sites;
- Setup logon passwords if you share a computer with others;
- Use a different password for social media sites from those you choose as your password for PAYMONT Internet Banking;
- Regularly check your privacy settings on social media sites such as Facebook. Don't accept requests from people you don't know;
- Never store any access codes on social media websites or respond to messages asking you to provide personal details or click on links to provide information.

For more information please

- **see the General Payment Services Agreement available at:**
  https://www.paymont.eu/wp-content/uploads/2022/07/PAYMONT_General_terms_ver.2022_07_15.pdf
  or
- call + 370 627 51 117 or +420 296 187 878
  or
- write us an e-mail at: support@paymont.eu