POSSIBLE FRAUD SCHEMES

THIS DOCUMENT SERVES FOR THE CUSTOMER´S AWARENESS OF POTENTIAL FRAUD AND SCAM SCHEMES

WHY DO I NEED TO READ ABOUT FRAUD AND/OR SCAM SCHEMES?

Fraudsters are getting more and more active, so you (or people close to you) might be their next target.

That is why you need to be aware of the main types of fraud and scam techniques being used.

Criminals are smart. You have to be smarter.

WHAT IS A FRAUD? WHAT IS A SCAM?

Fraud: criminals use techniques to obtain your account or card details, and use those details to make transactions without your knowledge.

Scam: criminals trick you into making a transaction you suspect to be real, while this transaction is instead for their benefit. This typically comes from them pretending to be someone they are not.

WHAT ARE THE MOST POPULAR TYPES OF FINANCIAL FRAUD TO BE AWARE OF?

Criminals are using sophisticated techniques to trick people and steal their money. Here is a list of some, but not all, of the fraud and scam techniques you need to be aware of:

- Bank transfer scams, or authorised push payment (APP) fraud, including:
  - Investment scams & Ponzi schemes
  - Charity scams
  - Romance scams
  - Impersonation scams
- Financial account takeovers
- Remote support, or installation of software fraud
- Delivery fee/Customs fraud
- CEO fraud

Bank transfer scams, or authorised push payment (APP) fraud

Bank transfer scam is when criminals trick you or use persuasion to get you to transfer money to another account. Such scams have increased dramatically since the last few years. The most common forms are:

- Investment scams & Ponzi schemes, when criminals convince their victims to move their money to a fake fund or to pay for a fictitious investment.

  These days it can be difficult to distinguish a sophisticated scam from a genuine investment opportunity.

  It can be hard to spot fake websites, ads, reviews, emails and text messages when they look and sound like legitimate investments. So here's our guide on how to spot a scam.

  Signs of a potential investment scam:

  - Social media ads offering suspiciously fast and high returns on investments with little or no risk, even if they appear to be promoted by a well-known celebrity, influencer, or even government agency.
  - When someone contacts you out of the blue by phone, email or social media about a potential investment opportunity.
  - You are pushed to make a quick investment decision without having time to consider your options.
  - You are told to download screen sharing or remote access tools to "support" you in the investment process. A legitimate financial institution would never ask you to do this.

  How to avoid an investment scam

  - Verify the existence of an investment company by checking the list of financial institutions and investment funds of the European Central Bank.
  - Search for the company name on the internet and call the phone number from independent sources. Look for any negative reviews or comments from other consumers regarding scams.
  - Reject so-called cold calls, in which traders call old contacts with whom they no longer maintain active contact. If someone calls or texts you

about an investment opportunity, it's safest to hang up and ignore any automated voicemail messages.
    - Be extremely cautious... Talk to a trusted family member or a friend, show them the investment opportunity, so they can help you verify its legitimacy. If you are not sure whether an investment is suitable for your individual situation, ask for professional advice from an authorized independent financial advisor before investing.

- Charity scam, when scammers will take advantage of your kind spirit and get you to donate to a cause you care about - but the funds go straight to them.

- Romance scams, when criminals claim to be romantically interested in you and take advantage of your emotions in order to convince you to send them your money.

- Impersonation scams, when scammers pretend to be from an organisation such as a bank, utility company, or tax authority. They might tell you there is something urgently wrong and you need to move your money. Often they'll emphasize that they need it quickly, or that there is a time limit.

Financial account takeovers

Typically, this kind of scam works because someone gains access to your email and password through phishing, a data breach, or an emerging cyber threat such as a man-in-the-middle attack where they steal your credentials while using public Wi-Fi.

Remote support or installation of software fraud

This type of fraud occurs when criminals ask you to download software, usually in the form of a mobile or desktop app that typically allows criminals to see your screen or take over your mouse, to gain access to your online or in-app account and transfer money. Fraudsters often use remote access software applications to gain control of your banking and finance applications.

Delivery fee/Customs fraud

Scammers know we're all addicted to shopping online and that we usually have important deliveries on the way! They'll text you and pretend a parcel is stuck in customs, or pretend a delivery has failed, in order to persuade you to provide important personal information.

CEO fraud

Businesses can also be the victims of fraud. CEO fraud is an increasingly popular means for criminals to persuade businesses to illicitly transfer funds. Scammers impersonate the CEO or other senior business leaders of your organisation and convince victims to make payments, again, often stating they need it urgently.

WHAT TO DO IF YOU NEED HELP?

You may need to take different actions depending on what financial fraud a criminal has committed under your name. But in all cases, you'll want to:

- Contact Paymont, and all other impacted companies and financial institutions.
- File a police report with local law enforcement.
- Freeze or cancel affected accounts.
- Set up a credit freeze or lock to stop further financial fraud.
- Review your credit report and dispute any fraudulent activity
- Change your account passwords and start using a password manager.

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, with regularly sent statements set up based on 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
- fraud@paymont.eu, or
- send us a message through your Internet Banking

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.

RECOMMENDATIONS 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 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
  or
- send us a message through your Internet Banking.