## General Provisions

The information listed below consists useful tips (the "Security Tips") for a more secure end-user experience related to some of the services and products provided by Unlimint EU Ltd (the "Company", "Unlimit").

For the avoidance of any doubt, the term "end-user" refers to customers of the Company (the "Customers", "you"). In addition, the term "Internet banking" shall have the same meaning as per Unlimit's General Terms and Conditions as well as Card Terms and Conditions.

We advise you to apply the following Security Tips, which are not exhaustive and therefore you are encouraged to take any additional reasonable steps you consider fit in order to avoid improper, insecure, fraudulent and illegal use of the Company's services, products and infrastructure.

Please note that the Company takes no responsibility as to any security breaches and consequences, including financial losses, if such has been caused by the actions and/or omissions of the Customers.

## Keeping your IBAN Account safe
## Payment (Current) Account Security Tips

- Protect your computer/laptop/smartphone/or other device from viruses and hackers. Make sure that you have installed anti-virus protection software and the latest antivirus updates/bases.
- Run a scan to check local/removable/network drives by antivirus regularly, once per week would be OK in case there were no incidents on your PC. Otherwise, do it right after the incident.
- Do not insert/connect your smartphones, flash drives and other removable devices (the "Devices") to unknown PCs/laptops/devices as viruses/malicious programs might be installed and transferred to your Devices.
- Never open/run *suspicious* links/sites/archives/programs including *suspicious* links/files received by email from well-known senders as your sender may have been hacked.
- Make sure you have enabled firewall on your operating system and it is configured to pass only authorized connections.
- Make sure you have installed the latest operating system updates.
- Make sure you have updated the operating system and antivirus bases frequently; you can use the automatic update mode.
- Lock the screen of your computer/laptop/smartphone/or other device if you need to leave your place. Also try to keep your computer/laptop/smartphone/or other device in safe place and do not leave it unattended in public areas.
- Configure Multi Factor Authentication ('MFA') known also as Two Factor Authentication ('2FA') if possible. All your services available to access from public internet should be protected by MFA, e.g. your web mail box, social media accounts, chat accounts etc.
- It would be advisable if your operating system is hardened according to the best security practices, for example CIS, security policy template is applied to your operating system.
- Check your Internet banking regularly.
- Use strong and complex passwords for accessing online banking.
- Change your password/passcode to Internet banking regularly.
- You may want to use appropriate tools/password managers to keep your account data (login, password, registration email, etc.) safe; never write a password on a paper, on your desktop etc., where third parties may gain access to it.

- Avoid using the same password for all bank/online accounts. As good practice, password should not contain your name/birthdate/initials or any other information that identifies you and/or your family. As good practice, you should avoid using at least previous 4 passwords.
- Ensure that your browser does not store information; instead you can turn off browsers autocomplete settings.
- Avoid connecting to public Wi-Fi networks if you use a laptop or mobile device for an online transaction. Access your accounts only when using networks with a secure wireless connection.
- Always check that the total amount of each transaction you intend to make is correct.
- Monitor your account frequently to ensure that any transaction posted corresponds to the transactions that you have made.
- Access Internet banking frequently to ensure that a transaction was posted correctly and if not, contact your Relationship/Account Manager immediately.
- Never disclose your login password or OTP codes to anyone, including Unlimit and its employees, since we do not need this information.
- Access your Internet banking by login to the website manually (where applicable), rather than by clicking on links that redirect you from one website to the other. Avoid clicking and accessing links through emails.
- Check for an encrypted connection. The website address shall start with https:// ('s' stands for secure) and shall contain the padlock symbol with 'Secure' or the unbroken key symbol. By double clicking on the padlock or key symbol, you will also get confirmation that the certificate is still valid.
- Never access Internet banking or process transactions in case you have a confirmation from the web browser about invalid certificate.
- Shred/destroy any statements/documents containing sensitive personal information using crosscut shredder. Shred files with sensitive information by using special shredding tools.

**In case of any suspicions of irregularity/security issues/fraud please contact us immediately by sending an email to your Relationship Manager/Account Manager in order to report the incident. You may also contact the Company by phone during Company's working hours for assistance.**

## Keeping your CARD safe
## Card Security Tips

- Treat your card like your cash.
- Keep your card safe and secure at all times and do not allow other persons to use it or make it available (intentionally or accidently) for other person to record/get know card data.
- Keep your PIN confidential and do disclose it to anyone.
- If you decide to write the PIN down, disguise it so that it is not recognizable and never write the PIN on anything that is kept with or near the card.
- Memorize the PIN as soon as you receive it and destroy the PIN message you received from Unlimit immediately.
- Only disclose the card number for the purpose of making a card transaction and make sure nobody is watching you when you enter your card data. It is acceptable to use not more than 6 first and last 4 card digits if there is a need to identify your card with Unlimit.
- It is recommended to generally avoid performing card-not-present (remote) transactions over phone conversations or via electronic messages. Additionally, you should never send your card details over email or social media, such as for example Facebook, Twitter, Cloud storages (e.g. Dropbox), messengers (e.g. Skype, Slack, Teams). Do not store card details that are not encrypted on removable storages (e.g. USB flash), notepads etc.
- Immediately report theft or loss of your card. If you suspect unauthorized use, block the card immediately using the block SMS-command and contact Unlimit immediately.

- Make sure your card is returned to you after each transaction.
- Use your card only on secured merchants /websites (avoid clicking on unsolicited emails or deal links and accessing websites that do not seem to be secure). Check the trustworthiness of the website online and do not rely only on the website reviews as these might be untrue. You can check that the payment page of an online retailer is secure if when executing a payment, the website address changes from http:// to https:// ('s' stands for secure). Also, the website browser shall contain the padlock symbol with 'Secure' or the unbroken key symbol. By double clicking on the padlock or key symbol, you will also get confirmation that the certificate is still valid.
- Avoid using your card in public (i.e. public computers).
- Be careful when you enter your PIN.
- Always collect your card/ATM receipts.
- Keep your cards away from devices with magnets.
- Avoid using your card in an ATM terminal if you notice anything unusual or suspicious or if you think it has been tampered with.
- Always shield your hand when you enter your pin number. Always cover the keypad when entering the PIN.
- Avoid disclosing your CVV2/CVC2 number over the phone or via email.
- Check the receipts against the transaction confirmations/statements.
- For online purchases, we strongly recommend that you use the card on websites of merchants that support 3DS. All our Cards support and are enrolled in 3DS authentication. 3DS provides greater security to internet transactions to protect your card from unauthorized use. Completion of transactions requires the use of a One-Time Password (OTP) and/or any other factor specified. Each OTP is specific for a particular transaction and is sent to your mobile phone number linked to the card.
- Shred/destroy any statements/documents containing sensitive personal information.
- Ensure that your browser does not store information; instead you can turn off browsers autocomplete settings.
- Avoid connecting to public Wi-Fi networks if you use a mobile device for an online transaction.
- Check the legitimacy of the apps that you are downloading. Never use apps that request access or information of your card/account.
- Always check that the total amount of each purchase/payment you make is correct before entering card data.
- When shopping/paying online, get a copy of both your order form and the merchant's terms and conditions. You should as good practice save screenshots of your purchase as well.
- Check your SMS confirmations (where applicable) after every transaction.
- Regularly check your card balance by using the SMS command/or Internet banking functions; we recommend that you check the available balance before each card transaction to monitor any unauthorized use.

**If you suspect unauthorized use/fraud or if your card has been lost or stolen you should:**

- **Block the card immediately using the block SMS-command by sending BLOCK XXXX (*replace XXXX with the last 4 digits of your card number and leave a space between BLOCK and the number*) to + 357 99 092 924 and;**
- **Contact us directly for assistance via the Internet banking (if applicable) or contact your Relationship/Account Manager. You will be provided with a form in order to report full details of the incident.**

## Not exhaustive list of examples of incidents that might give rise to suspicion

**Phishing**

Phishing is a common technique used by criminals to send emails requesting your password, bank details or other personal data. General characteristics of these types of emails:

(i) create the sense of urgency, (ii) contain grammatical mistakes, bad spelling, awkward language, missing words, (iii) include instructions to click on attachments, (iv) have the same template as the emails you receive from Unlimit, (v) contain a link to a website similar to Unlimit's website and/or the Internet banking interface, therefore by log-in/clicking they can steal your data etc. If you consider that an email is unsafe, **please contact us first**. During our regular communication, we will never request for confidential information (i.e. password, PIN).

**Malicious software**

Malicious software can have the form of a virus installed on your computer/laptop/smartphone/or other device without your approval and awareness that can steal your personal information (i.e. password/login credentials).

**Vishing**

If you receive a phone by someone pretending to be an employee of Unlimit/associate of Unlimit or an automated voice giving you instructions and requesting private information stating that there was an unusual activity detected on your card/account, then this might be a fraudster trying to steal information. During our regular communication, we will never request for confidential information (i.e. password, PIN) over the phone.

**Smishing**

If you receive text messages requesting your immediate attention and containing URL or phone number, avoid responding. Smishing messages might request you to call to a phone number that has an automated voice response; usually the actual phone number is not displayed or shown a code.