FUNDSTR

Online Security Guidelines

- Please remember that you must take all reasonable precautions to keep your details safe and prevent any unauthorised use of any security details. If any information forms part of your security details, you should therefore make sure that you do not disclose it to anyone else – see terms and conditions that apply to your account for more detail.
- Never send authentication data by email. Never disclose your login information. No one has the right to request you to provide your personal number and authentication mean by phone or email.
- Before you provide personal data or other important information online, you must make sure that it is a secure, encrypted connection between the browser and the server on which the website is hosted. It’s secure if:
    - There is a padlock (or lock) icon in the lower right corner of your computer screen or the URL starts with "https".
    - A locked padlock indicates that the current website has an encrypted connection.
    - It may also be advisable to click on the padlock to check the authenticity of the certificate before logging in.
    - If padlocks are missing or open, encryption is missing.
- Do not provide personal, credit, debit card or account numbers on a website that is not secure.
- Don't forget to sign out — both from the websites and the computer you've used.
- Update your computer, tablet and/or mobile phone’s operating system and browser frequently. Always adhere to the requirements or security alerts of the manufacturer of your phone device.
- Anti-virus protection software: With the help of malicious software often referred to as viruses or Trojans, scammers take control of your computer or have full visibility into what you are doing on it. In this way, they collect information that they use for illegal purposes. They can also direct you to fake pages even if you have entered a correct URL (so-called pharming). Therefore, avoid clicking on links you are not sure about and make sure to delete cookies regularly as well as update all your software and especially firewalls and virus protection continuously to make these kinds of attacks more difficult.

- We recommend not to use public computers or Wi-Fi for any personal matters like banking. If you have to use a public computer, for example in a library or internet café, you must take extra care as you don't know what's installed on the computer. For example, you don't know if the computer you're using has a working and up-to-date anti-virus program or if someone is monitoring and recording all activities on the computer.
- Make sure to have a backup copy of any valuable information you have, preferably on a physical device like a removable hard drive that you keep disconnected from your computer.
- Always protect your computer, phone, or tablet with a password or security code. Do not reveal the screen lock codes to other persons and do not allow to unlock your phone with other persons' biometric data. Avoid storing passwords or other sensitive information in your notes or messages.
- Always lock your devices when you leave them unattended. The login session is terminated when no activity happens for certain time period. You will be asked to re-enter your login details. Time limits are used for security reasons, to prevent internet banking access if a user forgets to log off from his/her account after finishing using the internet banking services. Once you finish session, log off (by clicking 'Logoff') and close the browser.
- Dispose of paper statements securely. When it comes to your personal details, it's not just online security you need to think about. Paper statements contain lots of information that's useful to criminals, so make sure you store them securely. Fraudsters may even search your dustbin for documents, so shred statements before throwing them away if you can.
- Remember, we'll never ask you to:
  - tell us your card's 4-digit PIN,
  - share your online banking password or Secure Key code,
  - send us your card or cash.

If you're contacted out of the blue by phone, email or text:

- stop - taking a moment to stop and think before parting with your money or information could keep you safe.
- challenge - could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- protect - check with someone you trust, such as a friend or family member and contact the company directly.

If you have authorised a payment and now believe you have been the victim of a scam, or you suspect you may have divulged your security details please contact us via the FUNDSTR online platform, email or phone straight away. You can also forward any suspicious emails or texts to us at compliance@fundstr.com. Please tell us if you notice anything unusual on your account. We'll help you to stay up-to-date with our latest security advice.

When shopping online, be prudent with your personal and financial data. Properly assess the threats, which you may encounter on the internet. We recommend to ensure protection of personal devices and always follow these safety tips:

- Shop in reliable shops only. Take a critical approach to unknown sellers and try to find out more information about their activity. Find out whether the website presents detailed contact data of its administrator (address, phone, email, etc.), and make sure it does not contain various errors in their links (additional words or letters, strange symbols), popup windows, advertisings, a great number of links instead of informative content.
- Be cautious about discounts. You have found a high-quality product offered at a particularly low price? Before making a payment order, be sure that the company that offers the product really exists and is trustworthy. Be careful about advertisements in social networks. They may lead you to a fake online shop.
- Safe shopping by card. When shopping in e-shops, the most common way of payment is by card. In this case you will have to indicate the details of your payment card. If an online shop participates in international security programmes, special logos such as “MasterCard SecureCode”, and “Verified by Visa” for Visa cards are used in this shop. You may be redirected to internet bank to confirm payment transaction by logging in.