CYBERSECURITY & IDENTITY THEFT

Cybersecurity is the process of applying security measures to prevent identity theft, and ensure the confidentiality, integrity, and availability of data.

Fenix Securities, LLC ("Fenix") takes cybersecurity and identity theft seriously and has implemented policies and procedures to control the dissemination of any personally identifiable information. Fenix has implemented procedural safeguards for access to and disclosure of such information. Fenix requires employees to confirm they are dealing only with those persons who are the actual client, whether over the phone or through electronic means. Fenix will not provide personally identifiable information over the phone or in an email without verifying the identity or email address as known to be that of the client, nor will employees take verbal instructions to make changes to a customer's existing information without such confirmation.

Fenix confirms in writing, to the last address or email in the client file, any changes made to an account. Therefore, it is important that customers review communications from Fenix and contact Fenix immediately if they did not authorize the changes to their account. Also, Fenix encourages clients to avoid falling victim to 'phishing' attempts: Do not provide information to anyone contacting you without verifying it is a Fenix employee. Hang up and call back your Fenix contact at the information on your statement if you have any doubt as to who you are speaking with.

PROTECTING YOUR ACCOUNT

Fenix encourages clients to take the following steps to help protect their accounts and personal information:

- Enable multi-factor authentication on the trading platform and on the email account associated with your Fenix account.
- Use strong, unique passwords and do not share them with anyone, including persons claiming to represent Fenix.
- Keep the devices used to access your account updated and protected with antivirus or endpoint security software.
- Avoid accessing your account from public or shared computers or unsecured Wi-Fi networks.

INCIDENT RESPONSE AND CUSTOMER NOTIFICATION

Fenix maintains a written incident response program reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information. Consistent with Regulation S-P, if Fenix determines that sensitive customer information has been, or is reasonably likely to have been, accessed or used without authorization, Fenix will notify affected customers as soon as practicable, and no later than 30 days after making that determination, except as otherwise permitted by applicable law.

REPORTING SUSPICIOUS ACTIVITY

If you suspect unauthorized access to your account, or receive a suspicious call, email, or message claiming to come from Fenix, please contact Fenix immediately at support@fenixsecurities.com