Account Funds Security Statement

In order to ensure the security of your trading account, please read the following instructions carefully and follow the recommendations.

1.Redstone Account Funds Security System

a. User Name

The user name you logged in to the Redstone website is the mobile phone number or email address you used to register. Please properly protect your mobile phone number/e-mail address and avoid unauthorized access!

b. Standard Security System-Password Login

When you log in to the Redstone trading account, you need to enter the user name and the password you set. Please ensure that your password is not leaked to ensure the security of your account funds.

c. Additional Security System-E-mail/SMS

1) During the registration process, you choose the following additional account security types: e-mail.

When performing balancing operations or changing account settings, we send an e-mail to the e-mail address you provided during the registration process. This email contains a unique code to confirm the required transaction. After the code is entered into the corresponding column in the Web site, the transaction is confirmed and executed.

E-mail confirmation of transactions is a lower level of security protection. If a hacker controls your e-mail account, he can access your personal area or transfer funds to other accounts. Be careful when using this security type.

If you receive an e-mail containing the code, but you do not perform any action in your personal area, please delete this e-mail immediately and report it to the technical support staff. Never provide confidential confirmation code to anyone.

2) In the registration process, you choose the following additional account security types: SMS.

When performing balance operations or changing account settings, we will send a short

message to the mobile phone number you provided during the registration process. This short message contains a unique code to confirm the required transaction. After the code is entered into the corresponding column in the website, the transaction is confirmed and executed.

If you cannot access your SIM card, you will not be able to change the security type.

2. Suggestions on the Protection of E-mail

a. It is recommended that you use an e-mail service with dual authentication.

b. It is recommended to delete security questions in your e-mail account security settings or use random characters as answers. Security Tip: Answering security questions is the most common way to hack e-mail accounts.

c. Log in to your email account with a secure password. Your password should not contain complete words, password length should be greater than 10 characters, should contain numbers and capital letters.

d. If you access related services through network interface, please disable SMTP, POP3 and IMAP protocols in your e-mail account settings. This can protect your email account from malicious attacks.

e. Do not click on suspicious links in e-mails from strangers or organizations! If you receive an email containing a link and click on the link, do not enter any password subsequently.

3. Suggestions on Account Security Protection

a. Never disclose the password logged into your personal zone to a third party to avoid hackers gaining access to the password.

Our technical support personnel do not have access to your personal zone, nor do they have the right to ask you for a password to log in to your personal zone. Company staff can only ask you for a telephone password that can be used to confirm your identity. To enable third parties to access a specific account (e.g., investor), use the investor's password for that account. This password does not allow you to change account settings, nor do you allow transactions or transfers of funds in your name.

b. Never disclose secret PIN codes received by SMS.

We strongly recommend using a separate file stored on a dedicated external media (USB flash disk, CD, etc.) in a secure area to save the password logged into your personal area and remove it from your computer.

4. How to Contact Us

If you suspect you have been cheated, please contact the technical support staff immediately by online inquiry (Live Chat) or e-mail support@redstonefx.com

According to our Customer Agreement, the following means of communication are allowed between customers and companies:

· E-mail (with @redstonefx.com domain name, such as support@redstone.com)

· The internal mail system of MetaTrader trading platform,

· The relevant telephone number can be found in the "Contact Us" section of the company's website.

· Mail,

· Online customer service.

Redstone's official communications do not use the following ways: ICQ, Yahoo Messenger, Skype, etc. Any e-mail sent by a domain name other than support@redstonefx.com is not our official communication, even if the e-mail address contains the word "redstone". The information provided by such e-mail addresses has nothing to do with us.

Dear customers, we hope that the above suggestions will be helpful to you. Redstone will do everything possible to ensure the safety of your funds. If you fail to comply with these security requirements, you should be aware that you are fully responsible for the security of your funds in your Redstone account.