Terms and Conditions regarding Communication by e-mail

These General Terms and Conditions regarding the Communication by e-mail form an integral part of the Agreement for Communication by E-mail concluded between the account holder/s, client(s) and contracting parties (hereinafter together the "Client") and Rothschild & Co Bank AG (the "Bank").

The Client and the Adressees/Senders herewith acknowledge the below information, terms and conditions when communicating by e-mail with the Bank. He/they is/are aware that there are certain threats in today's global communication environment and that it is key to securely handle her/his/its data regarding any banking activities.

Risks

The Client and the Adressees/Senders acknowledge that an order, notification or communication sent by E-mail is transmitted over an open, publicly accessible network and sometime across borders, and can therefore in principle, and if not encrypted, be seen by third parties, also allowing such third parties to infer that a banking relationship exists with the Bank. The Client and the Adressees/Senders also acknowledge that the linguistic and electronic content of an order, notification or communication sent by unencrypted E-mail may be changed and manipulated by third parties.

If the communication between the Bank and the Addressee/Sender is encrypted, the content of the communication with the E-mail addresses or domain name given will be protected. The Client and the Adressees/Senders take note that only the content is protected, but not the Bank’s E-mail address and the E-mail addresses or domain name given, these are not anonymous and the fact of the communication with the Bank remains therefore visible.

To this extent, the Client and the Adressees/Senders therefore expressly release the Bank from bank client confidentiality and data protection.

Furthermore, unauthorized persons could be capable of gaining unauthorized access to the IT facilities (the personal computer, for example) of the Client or the Addressee/Sender during the internet session. The Client and the Adressees/Senders are aware and acknowledge that such risk might be increased when indicating only or also a domain name. It is therefore the responsibility of each user to take all the appropriate technical precautions to minimise the risks inherent in using the internet and to ensure that the IT system is equipped with the latest defences against malware (e.g. viruses, worms, Trojans) and hackers (e.g. through use of a firewall).

The Client and the Adressees/Senders acknowledge that the transmission of an order, notification or communication may be delayed, interrupted or entirely prevented as a result of transmission errors, technical defects, outages, faults, illegal intervention, network overload, and wanton blockage of electronic access by third parties or other failures on the part of the network operators. Furthermore, delays may also occur in connection with the time used within the Bank to process an E-mail.

Identity theft

Identity theft is one of the fastest growing crimes in the financial industry affecting millions of people each year. Identity theft is the act of stealing someone’s identity/personal information, such as name, date of birth, address, e-mail, etc., which is then used by fraudsters for their financial gain. For instance, fraudsters can use identity details to execute payments and money transfers or use credit card information to buy goods and services at the expense of the individual whose identity has been stolen. A common way for fraudsters to obtain identities is by compromising an individual’s e-mail account and gaining access to e-mail correspondence, in order to identify the individual’s relationships and potentially exploit them.

Fraudulent e-mails

Fraudsters often use e-mail as a means to collect personal information from individuals. Such e-mails may request the recipient to update or to verify their personal and financial information, including date of birth, log-in information, account

details, credit card numbers, etc. Usually, these e-mails claim to come from a legitimate organisation such as a bank or online retailer. The e-mail contains a link that takes you to a fake website that looks identical (or very similar) to the organisation's genuine site. The fraudster can then capture personal data like passwords as you type it in or download malware onto your computer.

Should a Client or the Adressees/Senders receive any e-mail regarding banking specific requests where it is not sure if its source is in fact the Bank, the Client or the Adressees/Senders shall contact the Client Adviser by phone for verification. If the Client and the Adressees/Senders have any suspicion that an e-mail account from which there has been communicating with the Bank may have been compromised, the Client and the Adressees/Senders shall immediately inform the Bank.

Protection

To reduce the risk of having your e-mail account compromised or being a victim of identity theft, the Client and the Adressees/Senders are asked to observe the following security recommendations:

- Always remain on guard on the Internet and consider carefully to whom and where any personal data is disclosed.
- To not send passwords via e-mail, and to not share them with others. The Bank will never ask for a password.
- To not answer unsolicited or unwanted e-mails, and to not provide any bank account or personal details if asked to do so if there is no certainty about the recipient. The Bank will contact a Client or the Adressees/Senders only via the respective Client Adviser.
- To not click on any links in a suspicious e-mail. Clicking on such a link may cause the download of malware like a virus on the computer, which may allow a fraudster to gain access to personal information.
- Use a password that is difficult to guess to protect e-mail accounts. A strong password should consist of at least eight characters and include capital letters, numbers and special characters such as / $ _ # - + etc. Also, it is recommended to use separate passwords for different applications and accounts.
- Use antivirus software on personal computer and keep it up to date with new versions.
- Regularly review and reconcile statement balances to ensure that all transactions are legitimate. Similarly, always review account statements to check for unauthorized transfers.

The secure communication solution of the Bank

The Bank offers *Secure Email*, a secure environment for e-mail communication with the bank. *Secure Email* provides the Client with the following security benefits:

- E-mail correspondence with Rothschild is kept separated from your other personal e-mails and access to e-mails requires an additional username/password. As a result, a fraudster who has compromised your personal account would not have knowledge of your e-mails and information exchanged with Rothschild.
- e-mails of the Client or any Addressee/Sender are stored exclusively in the Bank's systems; they never leave the Bank's premises.
- The systems of the Bank are secure and subject to regular security reviews by specialized cybersecurity firms.
- *Secure Email* is easy to use and can be used on most devices.