Rahn+Bodmer
BANQUIERS SEIT 1750

Rahn+Bodmer Co.
Talstrasse 15
8022 Zürich
Telefon +41 44 639 11 11
www.rahnbodmer.ch

General Terms and Conditions for Rahn+Bodmer e-Banking

1. Scope of application

1.1. These General Terms and Conditions apply to the electronic services ("e-Banking") offered by Rahn+Bodmer Co. ("Bank"). They apply to all Clients who have entered into an e-Banking agreement with the Bank and any persons that the Client has authorised to use e-Banking (hereinafter referred to jointly as the "User").
1.2. The Bank reserves the right to issue further special provisions or enter further agreements for e-Banking services (such as the General Terms and Conditions of Business), which will take precedence over these Terms and Conditions.

2. Services offered

2.1. The services offered to the User include in particular access to his account and custody account information, a summary of his recorded transactions, and the option of sending and receiving information electronically. In addition, bank correspondence and other bank documents can be provided to the User electronically (cf. clause 5). **As a rule, neither stock exchange orders nor payment orders nor any other financial transactions may be recorded via e-Banking;** this is subject to any special arrangements made with the User.

3. Authentication procedure and access

3.1. The User may access e-Banking and the related services offered via the Internet (from Rahn+Bodmer Co.'s website or through the Rahn+Bodmer app, hereinafter referred to as the "App"), using any provider or mobile carrier he chooses. For this, he requires an internet-enabled end device and the necessary software, which he must obtain himself.
3.2. The User may choose to verify his identity for e-Banking through a multi-factor authentication process with a contract number, password and SMS code or TAN or through a one-step biometric identifier (such as touch ID or facial recognition). Biometric data can only be used with the App and its use depends on whether the User's device supports this function; if it does, authentication occurs only on the User's device and is thus outside the Bank's control. Where an SMS code is used for the authentication procedure, the access data are sent to the User's end device (mobile phone or other SMS-enabled device). If a TAN is used, the respective TAN will be displayed on the token that the Bank has provided.
3.3. The Bank regards any person who proves his identity in one of the ways mentioned above (self-identification) as a duly authorised User, who is entitled to full use of e-Banking and the related services offered; this applies even if such person is not the actual authorised user and irrespective of his internal legal relationship with the Client and/or the existence of any other contrary public documents or powers of attorney or signature arrangements. If, after the identification procedure has been duly carried out, e-Banking is used for any actions, notifications, etc., the Client will be responsible for these and be deemed to have authorised them, and will be legally bound by them.
3.4. The Bank will send security codes and devices to the address or phone number provided to it by the User. The Bank may add to, change or replace the security codes or devices at any time. The User acknowledges and agrees that the Bank is unable to control who accepts and uses the security codes or devices.
3.5. If the User enters his personalised security codes incorrectly three times, he will be locked out of e-Banking. A User who uses a password to identify himself may therefore block his own access to e-Banking by entering his security codes incorrectly three times. Similarly, the Client is entitled to block or revoke his attorney's access to e-Banking; if this occurs, e-Banking can only be unlocked upon request from the Client. Furthermore, every User is entitled to arrange during the Bank's business hours to have his access to e-Banking blocked.
3.6. The Bank is entitled to block the User's access without giving reasons and without prior notice and/or to require the User to identify himself in another manner (e.g. through signature).

4. Communication and electronic mailbox

4.1. The Bank provides the User with a secure and personalised internal messaging functionality for e-Banking. The purpose of this function is in particular to enable the User and the Bank's client advisor to send and receive confidential notifications and questions, for administrative matters or requests for quotations. The availability of this function may depend on the User's domicile or other factors relating to the User, which is why it may not be available at all or its use may be limited.
4.2 Notifications sent to the Bank are dealt with in the course of business during normal business hours on bank working days. **This function should not be used for orders or instructions that are time-critical or subject to a deadline** (such as stock exchange orders or payment orders, subscriptions to share issues, revocation of orders or powers of attorney or blocking of access to e-Banking). The Bank is entitled, but is under no obligation, to accept and execute instructions, orders or other notifications from the User, which it receives via this function, without waiting to receive possible confirmation in writing. However, the Bank accepts no liability for orders or instructions which are not executed on time or for loss or damage (particularly share price losses).
4.3. The Bank may use the User's electronic mailbox for serving notifications on him. **Such notifications are deemed duly delivered at the time that they can be accessed electronically in e-Banking.** The User is responsible for ensuring that he reads notifications sent to him in a timely manner.

5. Electronic delivery of documents

5.1. The User may instruct the Bank to deliver the records of his bank transactions or his entire bank correspondence (such as account / custody account statements, credit and debit advices, confirmations, bank statements, notices in connection with financial transactions, copies of agreements entered into with the Bank, hereinafter referred to collectively as "e-Documents") either exclusively or in addition to normal dispatch by post to his electronic

mailbox. **The same applies to key information documents, prospectus or other legally prescribed investor information.**
5.2. The Bank determines which documents may be made available electronically and reserves the right to amend this offer at any time.
5.3. e-Documents are deemed **to have been delivered at the time that they are received in the electronic mailbox and thus have the same legal effect as documents delivered by ordinary mail. Through electronic delivery, the Bank satisfies its notification and accountability duties**. This also applies even if the documents are also delivered by ordinary mail, the User does not access his e-Documents or he temporarily or permanently has no access to Rahn+Bodmer e-Banking. Time limits begin to run when the e-Documents are delivered in this manner (e.g. time limit for raising an objection).
5.4. The Bank may, at its discretion, change the method of delivery at any time and may deliver bank documents by ordinary mail. The User may, in an individual case, request the Bank to deliver additional documents by ordinary mail or in another manner. In such case, the Bank will be entitled to charge a fee in accordance with its conditions.
5.5. In correspondence with domestic and foreign authorities, e-Documents do not necessarily have probative value. For this reason, such documents may be ordered in paper form during the statutory retention period.
5.6. The User or the Bank may cancel the instructions for the delivery of e-Documents at any time. In this case, bank documents will again be delivered by ordinary mail.

6. Availability of notifications and e-Documents
6.1. Notifications and e-Documents will remain available in e-Banking for at least three years. The Bank reserves the right to remove read and unread notifications and/or e-Documents from e-Banking at the end of this period. Notifications and/or e-Documents will also be deleted where the account / custody account to which the e-Banking agreement relates is closed or the e-Banking agreement is cancelled. It is therefore in the User's own interest to access such notifications or e-Documents as required and to store them.

7. Notification services
7.1. The User may have the Bank notify him electronically (e.g. via e-mail or SMS) of certain events (new notifications in his electronic mailbox or receipt of new documents). However, the system is such that these messages are sent unencrypted through public communication channels. In addition, the Bank cannot guarantee that the User will receive the notification in every case and/or receive it on time.

8. Obligation on the part of the User to exercise due diligence
8.1. The User must adhere to the Bank's instructions regarding the use of e-Banking.
8.2. The User must connect to e-Banking exclusively by logging in via the Rahn+Bodmer Co.'s website or by using the Rahn+Bodmer App. He is not permitted to use links to establish a connection.
8.3. If the Bank issues the User with a password, he must change it immediately after he receives it and thereafter change it at regular intervals. The password must not consist of easily ascertainable combinations (e.g. birthday, car registration number, phone number, etc.) or strings of characters.
8.4. The User must keep his security codes carefully, secret and store them separately, and must protect them from misuse by unauthorised persons. In addition, he must protect his end device to ensure that no unauthorised persons access it.
8.5. **The Bank will never contact the User by phone, e-mail, SMS or any other media and ask him to disclose security codes or Bank data (risk of phishing e-mails).** The User must not click on links in attachments or suspicious e-mails. He must never follow up to such requests or enter his details on a website which does not have a Rahn+Bodmer Co. certificate! If the User notices upon the login any irregularities (e.g. the entry screen disappears briefly or he is rerouted to another website), he must cut the connection immediately and notify the Bank.
8.6. If there is reason to believe that unauthorised persons may have access to his security codes, the User must without delay change the respective password or inform the Bank so that it can, in any event, block access. The User must also inform the Bank without delay if he loses the means of identification that the Bank provided him with or if he loses his smartphone, tablet, etc. (if this is the device that he was using with the App for authentication purposes) or if the device is misused or used without authorisation; in this case, the User may go to the settings and block or delete his device in e-Banking himself.
8.7. The User is obliged to minimise security risks (e.g. always log out via the website menu and use anti-virus software). In addition, the User must regularly install security updates on his operating system and update all his programs and apps. The User is responsible for finding out about the necessary security precautions and for implementing them.
8.8. Except in the event of gross negligence on the part of the Bank, the Client is responsible for any damage arising from the disclosure or use – even illegitimate use – of his credentials or those of his attorney.

9. Security instructions
9.1. For security reasons or due to maintenance work, the Bank may, at any time and without prior notice to the User, cut off access to its e-Banking services or block the use of the software that it has provided on devices.
9.2. Even if data transferred during e-Banking are automatically encrypted, the sender and recipient are still unencrypted and the data are nonetheless transmitted over an open network that anyone can access. The User understands the risks involved in exchanging information and data over open and private networks and of the use of the hardware and software provided by the Bank, in particular the risk that the end device is outside the control of the Bank and that the use of apps on a mobile device or the delivery of security codes to such a device (e.g. delivery of a code via SMS) can lead to a third party inferring that a banking relationship exists or obtaining client information or inferring when and with whom the User has been in contact. The User uses e-Banking and the hardware and software which the Bank has provided at his own risk.
9.3. The authentication procedures (cf. clause 3) mean that the Client bears the risks arising from (i) manipulation of the User's IT system, (ii) misuse of his personal security codes or means of identification, (iii) a breach of due diligence duties or (iv) interference of unauthorised third parties in the transfer of data.
9.4. The User also understands that biometric authentication (through the App) is – compared to multi-factor authentication via the internet – a single-factor authentication process. In addition, the technology used is supplied by third parties. The Bank therefore has no influence over any security gaps in such technology.

The User uses this function at his own risk.

10. Warranty and liability

10.1. The Bank accepts no responsibility (i) for delays or interruptions in access to its e-Banking services or (ii) for the provider or mobile carrier or for software or for the User's end device.
10.2. The Bank accepts no responsibility for the accuracy or completeness of the data which it transmits via its e-Banking system. In particular, all information regarding accounts and custody accounts (balances, statements, transactions, etc.) and information contained therein, such as market prices and exchange rates is deemed to be provisional and non-binding.
10.3. Notwithstanding the use of the latest security technology, it is not possible to guarantee absolute security. To the extent permitted by law, the Bank excludes all liability for any direct or indirect damage or consequential damage which the User may incur as a result of transmission errors, technical faults, malfunctions, interruptions (including systems maintenance work) or network overloads at the Bank and unlawful or abusive interference or attacks on the Bank's networks or those of third-party providers, malicious blocking of electronic access, Internet malfunctions or other equivalent occurrences.
10.4. The Bank accepts no responsibility or liability for the User's end device, his technical access to e-Banking, the software he needs for this (including the download of the App) or any manipulations or unlawful interference (phishing attacks, viruses, etc.) within the User's sphere of control.
10.5. Liability claims shall also be excluded if the circumstances giving rise to the claim are based on an unusual and unforeseeable event to which the party relying on this event has no influence and the consequences of which could not have been avoided by it despite due care being taken.

11. Conditions

11.1. The Bank reserves the right to introduce a fee for the use of e-Banking (including for the hardware provided) and the related functions at any time and/or to change same at any time. Changes will be notified to the Client in a suitable manner.

12. Power of attorney arrangements

12.1. The Bank reserves the right to make access to e-Banking and the related services subject to the Client's separate grant of a power of attorney to his attorney. If this power of attorney is revoked or expires, this will automatically result in the cancellation of the attorney's access to e-Banking. On the other hand, the blocking or revocation of the attorney's e-Banking access alone does not lead to the revocation of the Client's existing power of attorney.

13. Bank-client confidentiality / data protection

13.1. The User understands that electronic communications (such as messages sent via SMS or e-mail or the delivery of security codes via SMS) are not encrypted. A third party could intercept and view such data. Data that are transmitted via e-Banking are encrypted, but they are nonetheless transmitted over an open network that anyone can access. The sender and recipient remain unencrypted resp. visible in the case of every communication. It is therefore possible for third parties to infer that a banking relationship exists; this is the case particularly where the App is used (e.g. provider of the application software). In addition, it is possible that data may be transferred across borders even if the sender and the recipient are both located in Switzerland. The Bank is therefore unable to fully guarantee bank-client confidentiality or the confidentiality of notifications or documents that are transferred over open networks of such kind or over networks of third party providers.
13.2. The principles relating to "How Rahn+Bodmer Co. process data" also apply to e-Banking and the functions which it offers, and to the data obtained (these can be obtained via the website of Rahn+Bodmer Co. or from the client advisor).

14. Foreign laws

14.1. The use of e-Banking from abroad and, if applicable, the means of access made available by the Bank may in some certain circumstances violate rules of foreign law. The User is responsible for informing himself about any such restrictions. To avoid legal risks in cross-border banking, the Bank expressly reserves the right not to offer or to limit its offer of e-Banking to Users domiciled or resident abroad. The Bank accepts no liability in this respect. The foregoing is without prejudice to any legal or regulatory provisions which govern the operation and the use of the Internet.

15. Termination

15.1. The Rahn+Bodmer e-Banking agreement may be terminated at any time and without notice by either the User or the Bank. If the agreement is terminated, the User must return to the Bank the means of identification that it provided him with.

16. Amendments to the agreement

16.1. The Bank reserves the right to amend, at any time, these General Terms and Conditions and the services offered. Amendments will be notified by appropriate means to the User and shall be deemed accepted without objection within 30 calendar days of notification, but in any event, with the User's next use of e-Banking.