Van Lanschot

General Terms and Conditions for the Use of E-Banking

1 Area of Validity/Hierarchy of Terms

1.1 The General Terms and Conditions for the Use of E-Banking (hereinafter called "GTC E-Banking") apply to all e-banking services provided by F. van Lanschot Bankiers (Schweiz) AG (hereinafter called "Bank").

1.2 Furthermore for each e-banking service the respective Special Conditions and/or Terms and Conditions of Use (if any pertain to the respective service), the Bank's General Terms and Conditions, as well as respective terms and conditions provided on the Bank's website apply. In the case of objections the terms apply in the following hierarchy: (1.) Special Conditions/Special Conditions of Use, (2.) GTC E-Banking, (3.) General Terms and Conditions, (4.) Terms and Conditions for Internet Use (the Bank's website).

1.3 The data exchange regulated by the GTC E-Banking applies to banking transactions, etc., which have their basis in separate contracts or business conditions (e.g., General Terms and Conditions, General Terms and Conditions for Safe Deposits, Terms and Conditions for Payment Transactions, etc.). Within the scope for e-banking services in the case of deviant rules the present terms precede the aforementioned contracts or the Bank's General Terms and Conditions.

2 Range of Services

E-banking services offered by the Bank enable the Client to execute certain banking transactions online and to communicate with the Bank electronically. With e-banking the Client can draw up account and safe-keeping account information, as well as implement payment orders and has access to electronic information and documents. Further details concerning e-banking services can be found on the Bank's website. The Bank reserves the right to change its service offer at any given time. Changes will be communicated properly and are regarded as valid without objections within 30 days after notification.

3 Access to E-Banking Services/Legitimisation

3.1 The Client's or authorised User's (hereinafter called "User") technical access to e-banking services occurs with the User's device and the User's provider (e.g. Internet access provider, telecommunication providers, etc.) chosen by himself. The term "device" encompasses hereinafter all soft- and hardware (including mobile devices, mobile phones and other technical devices) used for the access to e-banking services. In order to use e-banking services the User's device must comply with requirements listed on the Bank's website at all times.

3.2 Access to e-banking services is available to anyone who is legitimatised for use by entry of valid legitimisation data for this service. Currently the following legitimisation data are valid:

a) The contract number given to the User by the Bank; **and**
b) User's self chosen password; **and**
c) An identification token provided by the Bank. The Bank is allowed to introduce further identification tokens or to withdraw existing ones at any time. Currently the following are valid:
   - Security Code List, which the User is provided with by the Bank; **or**
   - CrontoSign Swiss Application, which the User installs on his device of choice; **or**
   - CrontoSign reading device, which the Bank provides the User with.

Directions to use the legitimisation medium can be found in the instructions which the Bank provides the User with when the legitimisation medium is delivered and can also be found on the Bank's website.

In the case that the User uses CrontoSign Swiss Application or CrontoSign legitimisation devices he acknowledges and accepts that when the legitimisation device is activated for the first time it will be allocated with an identification number which will be saved in the banking system, as well as on the User's device (mobile phone or CrontoSign reading device) in order to identify the devices (mobile phone or CrontoSign reading device). **In the event that the User loses or replaces his mobile phone or CrontoSign reading device, then he is obligated to notify the Bank of this immediately and must order a new activation code for the new device (mobile telephone or CrontoSign reading device). The User herewith accepts that until the activation of the new device, all e-banking services cannot be used.**

The directions are effective and accepted by the User with the first use of the respective legitimisation medium. The Bank reserves the right to replace or adapt the legitimisation medium at any time due to functional reasons, of which the User will be notified in a timely manner.

3.3 With the entry of a valid contract number, as well as a valid password, which are part of the double-staged login process for security reasons, the Bank is authorised to provide the User's name/company name to specified third parties.

3.4 Whoever legitimises himself according to §3.2 (self legitimisation) is considered by the Bank as authorised to use e-banking services. Thus the Bank may, within limits of the services invoked by the User and without further verification of his authorisation, have access to e.g. investigations or the receipt of orders and legally-binding communication; This also applies if this person is not the true authorised User. **The Client implicitly accepts all transactions, which are implemented within e-banking services with the use of his legitimatisation medium or that of authorised Users. Likewise all instructions, orders and all communication received by the Bank per e-banking are regarded as entered and authorised by the Client.**

3.5 However, for security reasons and in the case of justifiable doubts the Bank has the right to deny the execution of services and to insist that the User identifies himself in another way (e.g. telephone number, date of birth, liscence plate number, etc.).

4 User's Due Diligence

4.1 In connection with legitimisation medium

Each User is obligated to **change the first password given to him by the Bank after receipt and it must be changed regularly thereafter.** The password must not be easily ascertainable (e.g. telephone number, date of birth, liscence plate, etc.)

The User must ensure that all legitimisation medium are kept secret and protected against misuse by unauthorised parties. Especially passwords may not be kept unsecured on the User's device or recorded anywhere else. Furthermore, legitimisation devices may not be passed on to third parties or made easily accessible in any other way (e.g. E-mails, that are allegedly from the Bank and prompt the User to enter his identification data or contain links to the Bank's e-banking login site, aka. "phishing-mails", must remain unanswered and deleted immediately). The User must also ensure that the directions provided to him with the respective legitimisation medium are followed.

In the case of suspicion that **unauthorised third parties have access to the User's legitimisation medium**, the User **must change the respective legitimisation medium immediately**. If this is not possible, then the User **must have the access to the respective e-banking services blocked immediately**.

4.2 In connection with the User's device

The User is obligated to minimise the risk of unauthorised access to his device (e.g. by use of public electronic networks such as the internet) by use of appropriate security measures. Especially operating software and browsers must be kept up-to-date, which means that the User must promptly install software updates and security corrections provided and recommended by the respective provider. Also security measures must be taken for the use of public electronic networks, such as the use of an anti-virus program or the installation of a firewall, which continuously have to be kept updated. It is the User's responsibility to stay informed about the necessary security measures which cater to the current state of technology, as well as to stay informed about the Bank's recommended security notices, which can be found on its website, and to implement the recommended security measures.

In the case of suspicion that unauthorised third parties have access to the User's device (e.g. computer), then the User is obligated to notify the Bank immediately (§19).

4.3 In connection with data entry

The User is responsible for the completeness and validity of all data entered by himself. The responsibility for the completeness and validity of the Data sent by the User remains with the User until these are taken over by the Bank's system.

If the User has sent an order (e.g. payment order, message, etc.) to the Bank electronically and afterwards the client establishes that the order has not yet or only partially been executed by the Bank, then the User is obligated to place a complaint immediately with the Bank. The Bank recommends that the User contact the respective relationship manager at the Bank in the case of uncertainties regarding an order's status (§19).

5 Confirmation of Transaction

To increase security the Bank reserves the right to require a transaction confirmation from the User for the confirmation of an order. In this case the User is obligated to compare the selected Data via CrontoSign with the original confirmation and to verify its correctness. If the data selected by the Bank is correct, the User must confirm the order (e.g. by entry of confirmation code), provided the User wishes to place his order with the Bank. If the data transmitted by the Bank is incorrect according to the User, then the User is obligated to cancel the transaction. If a transaction confirmation does not follow on behalf of the User, then the order is considered unplaced and therefore will not be processed by the Bank. Furthermore, the Bank is authorised, however not obligated, to implement a call back at its own volition.

6 Blocking of Services

6.1 The User can have his access to the Bank's e-banking services blocked. The blocking of electronic services can be requested over the Bank's hotline (§19) and must be confirmed immediately in writing. Furthermore the User can block his access to e-banking services at any time himself by entering the incorrect legitimisation data until the automatic blocking takes place (e.g. numerous entries of incorrect passwords).

6.2 The blocking can only be revoked with the Client's written request.

6.3 The Bank is authorised to block the User's access to single or all e-banking services at all times without the indication of reason or prior termination. This especially applies in the cases of §11.1 (Foreign Restrictions) and §12.1 (Security Risks/Maintenance Work).

6.4 For the prevention of dormant accounts the Bank has the right to record and analyse the User's access data. The Bank reserves the right to either contact the User or block his access without prior notification in the case of lack of use of e-banking services.

7 Risks

7.1 The Client is liable for all risks from the legitimisation understanding/breach of due diligence due to the legitimisation understanding according to §3.4. and for all consequences that result due to the – even misused – use of his legitimisation medium or the same for an authorised person (e.g. the unauthorised access of a third party), except if the Bank has breached its standard diligence. Furthermore the Client is liable for the consequences resulting from the breach of the User's due diligence according to §4 or the User's breaching of his verification duties regarding placed transactions and transaction confirmations according to §5. Additionally with the use of e-banking services the Client accepts the following risks (§7.2):

7.2 Public and private data transmission networks for data and information exchange, as well as the User's device are part of the overall system, over which however the Bank has no control. These can become a weak point of the system. They can especially become subject to the access of unauthorised third parties or transmission errors, delays, as well as system breaches or system failures can occur. **The Client cannot derive any claims against the Bank.**

8 Payment Orders

8.1 The User acknowledges, that the accounts for which the Bank was granted discretionary mandates with, are only limitedly accessible for the User. In particular no payment orders can be places via e-banking over these accounts.

8.2 Furthermore the User acknowledges that due to security reasons, per day and per currency account a maximum of CHF 100'000 (or equivalent) can be transferred. Once this maximum has been reached, no further orders can be placed. This limit can be raised with a written request from the Client.

8.3 Payment orders cannot be executed at all times, however only during the Bank's normal business hours.

8.4 When the User places a payment order he is obligated to comply with the applicable standards of the relevant transaction (e.g. domestic payments, foreign payments, etc.). In addition, the User acknowledges that in this respect all payment orders are executed without personal consultation with the Bank. The user herewith confirms that he is familiar with the customs and practices of payment orders and is aware of the risks of each transaction type.

8.5 For the execution of payment orders the Bank is authorised and commissioned to reduce or sell security positions, time deposits or fiduciary investments and in the case of insufficient currency execute relevant currency transactions. Furthermore the Bank is authorised to adjust the execution date without previously informing the User.

8.6 The Bank is authorised to reject or cancel payment orders if there are not sufficient funds (provisory §7.4) or it does not comply with the relevant standards of the respective transaction type.

9 Stock Exchange Orders

The User accepts that regardless of the account type, no stock exchange orders can be placed via e-banking. Stock exchange orders can only be placed in written form or per telephone with the Bank during work hours.

10 Secure Mail

10.1 The Client commissions the Bank to send him, respectively his authorised Users correspondence electronically via e-banking (function Secure Mail). Therefore the Bank is authorised to grant the User access to correspondence.

10.2 Electronic correspondence is considered duly received by the Client on the day on which it is available via the Bank's electronic services, which provide access to the Secure Mail function.

10.3 The Client agrees to view and acknowledge the available correspondence, notices and documents on a regular basis.

10.4 Thus the Client expressly acknowledges that with the electronic delivery of correspondence the Bank has complied with §10.1 and has fulfilled its obligation to notify the client.

10.5 However, the Bank is entitled to deliver correspondence in paper form via mail at any time without giving reason.

11 Electronic Acceptance of Special Terms/Legal Guidelines and Risk Investigations

11.1 For individual e-banking services there are special terms, which must be accepted before their use. The Bank may submit these terms in electronic form to the User. The User decides whether he wishes to use the respective services according to the applicable

terms by means of an input mask which submits an application to the Bank (if necessary) and consents to the terms for electronic services electronically. The User's consent is binding for both the Client (as owner of the account and safekeeping account) and for authorised Users. Electronically signed terms have equal validity to handwritten contracts.

11.2 Furthermore the Bank must include legal or risk advice in its individual e-banking services and/or published information. With the display of these notices and advice it is binding for both the Client and authorised Users to adhere to them. If he choses to not accept them, then he must forgo the respective service or information.

12 Foreign Laws/Import and Export Restrictions

12.1 The offer of e-banking services for users abroad can be subject locally to legal restrictions, which can lead to limitations of the offered services. The Bank is authorised at any time to change, restrict or fully cease the offer abroad of available e-banking services without giving notice.

12.2 The User acknowledges that with the use of e-banking services abroad he may violate sanctions or existing import and export restrictions (especially the identification medium and the encrypting algorithms contained therein) or other foreign laws. It is the User's responsibility to be informed thereof. In dubious cases it is best to waive the use of e-banking services, which are accompanied with the import/export of legitimisation medium. The Bank disclaims all liability in this regard.

13 Exclusion of Liability and Guarantee

13.1 The Bank cannot guarantee undisturbed or uninterrupted access to e-banking services at all times. The Bank reserves the right to interrupt e-banking services for the protection against security risks. Furthermore the Bank is authorised to interrupt e-banking services for maintenance work. Various damage caused by eventual breakdowns, interruptions or blockages according to §6.3 are borne by the Client, unless the Bank has violated corporate diligence. In case of failure, an interruption or the blocking of e-banking services the User must contact the relationship manager, respectively the Bank, directly by use of other available contact channels for the placement of orders or notices.

13.2 The Bank applies customary corporate diligence for the display and transmission of information, transferred data, communication, etc. (hereinafter "data") as part of its services. The Bank excludes any further warranty or liability for the correctness, completeness and actuality of data. In particular information concerning accounts and custody account (balances, statements, transactions, etc.), as well a publicly available information, such as foreign exchange rates are provisional and unbinding, unless they are expressly specified as binding. Likewise data set in services are only then binding offers only if designated as such.

13.3 In those areas in which the Bank vouches for the provision of its services with due diligence, it is only liable for direct and immediate damages to the Client. Liability for indirect or consequential damage to the Client is excluded.

13.4 The Client must check for and notify the Bank of potential damage of the hard- and software provided to the Client by the Bank (e.g. CrontoSign Swiss Application & CrontoSign reading device). If no such complaint is made with the Bank, then the hard- and software shall be deemed approved by the Client. For timely reported defects which affect the use of e-banking services significantly, the Client is only entitled to the replacement for the faulty hard- or software. The Bank also disclaims all warranty and liability for the correctness of the hardware and software and for the application thereof in combination with other systems chosen by the User or other third parties. In case the User identifies deficiencies in the hard- or software, he must immediately refrain from the use of e-banking services and notify the Bank thereof.

14 Terms of Authorization/Power of Attorney

14.1 The Client is obligated to inform the authorised User of the contents of this GTC E-Banking and to ensure that they comply with the obligations in the GTC E-Banking (in particular §4).

14.2 The power of attorney and proxy for the use of e-banking services is valid until the Bank has received written revocation thereof (§19). It is expressly determined that in the case of the Client's death or his loss of capacity to act the power of attorney does not expire, but until revoked in writing regardless of other entries is still valid in the trade registry and other publications. The withdrawal simultaneously terminates the contractual agreement between the Bank and the power of attorney regarding the use of e-banking services for the Client's account/custody account.

14.3 The deletion of a power of attorney's subscription rights to the Client's signed documents held with the Bank is not automatically followed by the repeal of its authority to use e-banking services. This requires a separate, explicit revocation as defined in §14.2.

15 Data Privacy/Banking Secrecy/Marketing

15.1 General Information

The User acknowledges that his data, especially payment orders are disclosed to domestic and foreign financial institutions, system administrators (especially telecommunication companies and commissioned third parties) and domestic, as well as foreign beneficiaries. Furthermore the Client acknowledges that data transmitted abroad is no longer protected by Swiss law (banking secrecy, data protection, etc.) and subject to the laws of the respective country. Due to the encryption used in e-banking it is almost impossible for an unauthorised party to view confidential client data. However, it cannot completely be ruled out that

transmitted data is completely secure from the access of unauthorised third parties. The User acknowledges that the device identification features (§3.2) are saved by the application CrontoSwiss Application and can be viewed by the application manufacturers as well as mobile phone manufacturers. Therefore the conclusion of an existing banking relationship by third parties (e.g. application manufacturers, mobile phone manufacturers) is possible.

15.2 Internet/E-Mail, etc.

With the use of an open, public network (e.g. internet, e-mail) for the transmission of data, data can be transmitted abroad uncontrollably, even when both sender and receiver are in Switzerland. Bank information, which the User receives separately – outside of e-banking – via e-mail, etc. are normally transmitted unencrypted, which is why banking secrecy and data protection are no longer guaranteed. Even with encrypted transmission both the sender and receiver are unencrypted. The conclusion of an existing banking relationship can therefore be made by third parties (e.g. the internet provider).

15.3 Marketing

The User consents that the Bank may use data derived from e-banking services used by him for internal marketing purposes.

16 Amendment of Terms

The Bank reserves the right to make amendments to the GTC E-Banking, to special conditions, respectively terms of use for e-banking services, as well as terms for eventually existing websites at any time. Such an amendment will be communicated to the Client for himself and his authorised Users by electronic advice or a message via e-banking or via another suitable channel and is considered approved within 30 days after notification without any objections

17 Termination

The termination of use of the Bank's e-banking services can take place on behalf of the Client and/or the Bank at any time without the adherence to a cancellation period (§19).

18 Partial Nullity

The invalidity, illegality or lack of enforceability of one or more terms does not affect the validity of the remaining terms.

19 Applicable Law and Place of Jurisdiction

All legal relations between the User and the Bank are subject to Swiss law. Place of fulfilment, place of prosecution for Users with foreign domiciles, and the exclusive venue for all other types of proceedings is Zurich – provisory of any other mandatory terms regarding place of jurisdiction in favour of the User. Furthermore the Bank has the right to prosecute the User at any other responsible jurisdiction or place of prosecution.

20 Contact

The hotline number (including blocking services) and the Bank's correspondence address can be found on all of its statements, as well as on the e-banking website. The hotline is available during normal business hours or during the service hours listed on the website.