

# VIRTUAL CORPORATE SOLUTION APPLICATION.

We wish to apply for a Virtual Corporate Solution (VCS).



**Important:** please fill out the application form and return it to us.

## 1. Company/Contact Person

Company name \_\_\_\_\_

Contact person \_\_\_\_\_

Phone \_\_\_\_\_ Fax \_\_\_\_\_

E-mail \_\_\_\_\_ Correspondence in:  E  G  F  I

### Personalized additional information:

Yes, we would like to be contacted by Cornèr Bank Ltd. with regard to our payment details.

## 2. Account Details

Desired spending limit per month (CHF):

□ □ □ □ □ □

Expected annual turnover (CHF):

□ □ □ □ □ □ □ □

## 3. Identification of the beneficial owner (form A pursuant to CDB 16, as required by law)

No information is required if:

- the assets used to conduct transactions with the prepaid card, and/or to settle the monthly credit card statements, and/or collected by the card issuer above this amount belong **solely** to the Company **and**
- the said Company is not a sole proprietorship or a simple partnership.

If this is not the case, the Company declares that these assets (please tick only one answer as appropriate)

- belong to the Cardholder.
- are held in trust by the Company for the benefit of the person(s) listed below:
- belong to the person(s) listed below:

(Last name(s) / first name(s) / date of birth / place of birth / nationality / home address incl. country)

\_\_\_\_\_  
\_\_\_\_\_

The Company undertakes to disclose any changes with regard to the card issuer on its own initiative. It is a criminal offence to deliberately provide false information on this form (Art. 251 of the Swiss Penal Code, document forgery; penalty: custodial sentence not exceeding five years or monetary penalty).

## 4. Online Services

E-Account access  
Card management at a mouse click.

Diners Club T&E Analyzer®  
The free and compact solution for small and medium-sized businesses to simply analyze and control travel costs.

Management Information System Global Vision®  
An exceptional and effective reporting solution designed for global corporations to analyze and control travel costs. Please send us further information.

Access to online services requires:

Last name \_\_\_\_\_

First name \_\_\_\_\_

Date of birth \_\_\_\_\_

Place of birth \_\_\_\_\_

E-mail \_\_\_\_\_

Mobile Phone \_\_\_\_\_

## 5. Declaration

The Company hereby certifies the information provided in this application to be accurate and acknowledges that it has received, understood, and accepted as binding the Terms and Conditions for the Virtual Corporate Solution portal (hereinafter referred to as the "VCS Portal") as well as the **General Terms and Conditions** (hereinafter referred to as the "GTC") for the underlying product, the Diners Club Corporate Travel Account (hereinafter referred to as the "CTA"), and the Diners Club Corporate Cards from Cornèr Bank Ltd. (hereinafter referred to as the "Bank"), issued by Cornèrcard. **The Company is liable** for all obligations resulting from the use of the VCS Portal. **The use** of the VCS Portal beyond the spending limit defined by the Bank is unlawful. In such an event, the Company shall repay the excess amount immediately and in full. The Bank is authorized to obtain any information it deems necessary about the Company. It may decline this application at its discretion without giving reasons. Upon acceptance of this application, the Company will receive the access credentials to the VCS Portal, it applied for, a copy of the VCS Portal application, and the complete GTC (which may be accessed at any time by visiting [dinersclub.ch](http://dinersclub.ch) or by telephoning +41 58 880 88 00). The conditions of insurance that apply to coverage provided automatically and at no charge with the CTA or provided upon request and for a fee can be accessed any time at [dinersclub.ch/firststep](http://dinersclub.ch/firststep). Any applicable premiums will be charged directly to the Card. By using the VCS Portal/CTA, the Company acknowledges that it has received, understood, and accepted in full the **VCS Portal/CTA Terms and Conditions** and the **GTC** as well as the applicable **conditions of insurance**.

**Charges, interest rates and fees:** The Company may be required to pay charges, interest, and fees in connection with the use and administration of the VCS Portal/CTA. The Company will be sent a schedule of "Charges, Interest Rates, and Fees" advising it thereof together with the enclosed application and/or by some other suitable means. Information on charges, interest rates, and fees may be accessed at any time by visiting [dinersclub.ch](http://dinersclub.ch) or by telephoning +41 58 880 88 00.

Any third-party charges and any costs incurred will also be chargeable. The Company acknowledges that it **accepts these charges, interest rates, and fees without reservation**.

**Exchange rates:** Transactions conducted in foreign currency will be converted at the retail exchange rate of the Bank on the booking date, plus foreign currency processing fees. **Authorization:** The Company authorizes Cornèr Bank to store, process, use, and analyze its contract and transaction data in order to compile customer profiles and to process them for marketing and market research purposes. This enables the Company to benefit from customized support and to receive tailored offers and information about available products and services from the Bank. **Insurance mediation and data protection:** The Company acknowledges that the insurer alone is liable for any errors, negligence, or incorrect information in connection with the insurance contracts provided. Personal data made available in relation to the insurance contracts may be disclosed to the insurers and will be processed by the Bank and the insurers only for the purpose of concluding and administering the insurance contract and in the event of a claim. Personal data may be disclosed to authorized third parties and/or other Group companies of the Bank for the purpose of processing the insurance contract. Data may be transferred abroad if such third country provides for equivalent data protection (recognized as such by Swiss data protection legislation). The Bank is entitled to commission third parties in Switzerland or abroad to perform, in full or in part, all services pertaining to the contractual relationship, including reward and loyalty programs (for example application reviews, card manufacture, card personalization, contract management including the printing and dispatch of correspondence together with the monthly statements, online services, payment collections, client communications, credit risk calculations, payment processing, IT) and for the improvement of the risk models used in granting credit limits and fraud prevention. The Company authorizes the Bank to provide these third parties with the data necessary for the diligent performance of the tasks assigned to them and, if required, to transmit this data abroad for this purpose. Data is only disclosed if the recipients undertake to keep the data confidential, to maintain an appropriate level of data protection, and to ensure that any other contracting partners are also bound by this obligation. The Company acknowledges that data transferred abroad may not be subject to data protection or to an equivalent level of data protection to that under Swiss law. Personal data is stored in electronic form and/or paper form. Pursuant to data protection legislation, the Company may be entitled to obtain information and, on certain conditions, to have certain data stored at the Bank corrected, blocked, or deleted.

**The Company will find additional information concerning the data privacy policy of the Bank on [cornercard.ch](http://cornercard.ch).**  
**The Company recognizes Lugano to be the exclusive place of jurisdiction.**

## 6. Company Signature(s)


Place/Date \_\_\_\_\_

Last name \_\_\_\_\_

First name \_\_\_\_\_

Signature\* **X** \_\_\_\_\_

\* Authorized signature(s) as recorded in the commercial register (individual or joint signature).

Company stamp 

Last name \_\_\_\_\_

First name \_\_\_\_\_

Signature\* **X** \_\_\_\_\_

**Please complete, sign, and return the card application to:** Cornèr Bank Ltd., Cornèrcard, Via Canova 16, 6901 Lugano



## 7. Terms & Conditions Virtual Corporate Solution

General Terms and Conditions governing the use of Virtual Card Numbers (“VCN”) generated via the Virtual Corporate Solution portal (“VCS”) operated by DataFlexNet Limited, Stafford, United Kingdom (such system hereinafter referred to as “VCS Portal” or “Portal”).

These General Terms and Conditions (hereinafter the “Terms and Conditions”) set out the legal relationship between the company applying for administrator rights (hereinafter the “Company”) or the individuals authorized to use the VCS portal (hereinafter the “Administrator” or “User(s)”) and Cornèr Banca SA (hereinafter referred to as the “Bank”) with regard to use of the Portal and of VCN.

Condition precedent allowing the company’s access to the VCS-Portal is the execution of a binding framework agreement for the issuance of Cornèrcard Business Cards and the valid request for Diners Club Corporate Product.

### 1. General provisions concerning the Portal’s access; use of VCN; payment of charges

- 1.1. Upon request, the Bank shall grant the Company access to the VCS Portal for the generation of VCN to cover airline tickets, rail travel, vehicle rental, hotel reservations, and travel agent services (hereinafter referred to as “Travel Services”) and mail-order transactions by mail or fax, or over the telephone or Internet (hereinafter referred to as “card not present transactions” or “CNP Transactions”) provided the Company guarantees that it will meet its financial obligations resulting therefrom in a timely manner as agreed.
- 1.2. The Company or its designated travel agency, internal travel department, or airline branch office (hereinafter referred to as the “Travel Agent”) will receive access to the Portal, for the generation of VCN issued in the name of the Company, together with credentials and related information. The portal shall be used exclusively by persons explicitly authorized by the Company for the acquisition of Travel Services and CNP Transactions. The Company shall ensure that the person specifically responsible for the VCS Portal contacts the Bank to obtain the necessary information. No physical Diners Club Card will be issued or provided.
- 1.3. **The Company is fully responsible for the use of the Portal by the respective Travel Agent. It accepts these Terms and Conditions and also ensures compliance therewith by the Travel Agent. The Company is liable, in relation to the Bank, for all charges resulting from the use of the Portal. The generation of VCN and the activation of Users will be at the sole risk of the company. The Bank will not be held responsible for any incorrect charges made by the Travel Agent, the Company, or employees of the Company. Any complaints by the company against the Travel Agent in connection with Travel Services are to be directed exclusively to the Travel Agent and will not relieve the Company from its obligation to pay the charges to the Bank.**
- 1.4. The Company receives from the Bank a monthly invoice listing all charges. The invoice is due and payable upon receipt. If the invoice is not paid within 25 days from the date of invoice, the Bank will, as of the accounting date, charge an annual rate of interest on all transactions in accordance with the “Charges, Interest Rates, and Fees” table until all outstanding amounts have been settled. If payments are made to the Bank by direct debit (LSV), the Bank may disclose any information regarding the Company, the VCS, and total amounts of expenditure, which may be required by the applicable correspondent bank. In addition, the Bank reserves the right to charge for costs and expenses charged by third parties in connection with the VCN.
- 1.5. **The Company and the Travel Agent shall exercise utmost care in safeguarding the Portal’s access data and the VCN numbers created via the Portal as provided for in further detail in sections 2 ss. here below. If a VCN number or User’s Credentials are lost, stolen, or used without authorization within the Company, the Bank is to be notified immediately in writing by the Company or Travel Agent so that it can block VCN and User credentials.** The Bank reserves the right to require the Company or Travel Agent to file a police report. Until such notice has been received by the Bank, the Company is liable for all unpaid invoices, transactions, and charges resulting from the use of the portal and the generated VCNs.
- 1.6. The Company may make use of the VCS Portal only to the extent that its financial situation is sufficiently sound to promptly pay all future monthly invoices. **The Bank reserves the right to block the Portal at its discretion and at any time** without the need to justify its decision. The Bank will not be held liable for any losses or damage suffered by the company as a result of such action. Each unauthorized use of an expired or blocked VCN is unlawful and may result in criminal prosecution.
- 1.7. The services provided via the Portal can be terminated at any time in writing by the Company or the Bank. Any charges posted to the VCN subsequent to such termination are to be paid immediately by the Company upon receipt of the next invoice in accordance with section 1.4 above.
- 1.8. The Company accepts that incentive program information with regard to transactions processed via VCN will be forwarded to the respective partner (such as the airline company). **The Company authorizes the Bank to collect from government agencies and designated bank or financial institutions any information deemed necessary by the Bank in connection with a VCS Portal application request or the use of VCN.**
- 1.9. The Company acknowledges and accepts that the Bank may commission third parties in Switzerland or abroad for the performance of contract-related services including premium and loyalty programs (such as application verification, card production and personalization, contract administration including printing and mailing of correspondence including monthly statements, online services, collection, communication with customers, assessment of credit risk, payment movements, IT) as well as improvement of risk models used in connection with fraud prevention. The Company authorizes the Bank to disclose to such third parties the data that are necessary to perform the tasks assigned to them and therefore to forward such data abroad as well. Such transfer of data shall occur only if the recipients are bound to maintain confidentiality or to guarantee appropriate data protection, and to extend such obligations to any other contract partners. Personal data are maintained in electronic and/or paper format.
- 1.10. Company data is stored in electronic form and/or paper form. The Company acknowledges that, under the data protection legislation, it may claim entitlements to information and, on certain conditions, request correction, blocking, or deletion of certain data stored at the Bank. The Company is entitled to have access to all information gathered about it by the Bank and to request correction of any data deemed to be false.

### 2. Authorization of Administrator and User to use VCS Portal

- 2.1. The Company authorizes the Administrator to activate other Users for the purpose of using the Portal.
- 2.2. The Company has overall responsibility for ensuring that all Users fully comply with these Terms and Conditions. Accordingly, the Company shall supply to each individual User detailed information on the Portal, the relevant functions, and the obligation of due diligence incumbent upon the User (see clauses 4 and 5 below).
- 2.3. Any authorizations conferred will not be invalidated automatically (for example due to death, incapacity to act, removal of signatory powers, deletion from a register, or termination of employment with the Company), but must be specifically blocked or canceled (see clause 6 below).

### 3. Personal identifiers

- 3.1. At the request of the Company, the Bank shall supply to Users their personal contract number and the applicable means of authentication, such as username and password (hereinafter referred to as the “Identifiers”). On logging in for the first time, Users must replace the password assigned by the Bank with their own personal password.
- 3.2. Users will gain access to the Portal and related services once they have been authenticated to the satisfaction of the Bank by means of the Identifiers.
- 3.3. The Bank may, at its discretion, change or replace the Identifiers at any time.

### 4. Authentication

- 4.1. **Any person who has been authenticated by entering Identifiers that are valid at the time of use, in accordance with Portal guidelines (self-authentication), are deemed by the Bank to be authorized to access the Portal and use the relevant services.** The foregoing applies irrespective of whether the person concerned is an actual User or has been authorized by the Company for such purpose. The Bank is deemed to have been appointed and authorized by the Company to execute orders received through the Portal, once the underlying authentication process has been properly completed.
- 4.2. Accordingly, the Bank is expressly released from any further obligation to verify whether an individual is in fact authorized to use the Portal, **irrespective of the relationship between the Bank and the User inter se, and the Bank is entitled to disregard any contrary provisions set forth in forms issued by the Bank, including, in particular, forms stipulating the signatory owners applying to the contractual relationship with the Bank (including card contracts).**
- 4.3. Notwithstanding the foregoing, the Bank is entitled to deny access to the Portal at any time, without giving any reasons, and to require Users to verify their identity by other means.
- 4.4. **Any transaction or act performed under the contractual relationship with the Bank (including card contracts) on the basis of prior authentication will be imputed to the Company, which duly and unconditionally agrees to any such transaction or act with binding legal effect.**

### 5. Obligation of due diligence

- 5.1. **The User shall take special care to ensure that the Identifiers are kept safely. Identifiers may not be sent, disclosed, or otherwise made accessible to other persons.** Personal passwords must be kept confidential and may not be noted down, stored electronically, or readily identifiable (no telephone numbers, dates of birth, car registration numbers, or number sequences that can be easily guessed, etc.) and must meet the Bank’s requirements in terms of integrity and complexity. The password selected will expire automatically in accordance with the rules defined by the Bank and must therefore be renewed and replaced at regular intervals.
- 5.2. Furthermore, Users shall take all practicable security measures to protect their workstation and, in particular, electronic data processing system (computer system and any data stored thereon), which are used to access the Portal, against unauthorized access, unauthorized use, and tampering or hacking (for example by deploying the latest firewall and antivirus programs). **The Company and the User shall obtain detailed information on any security measures required to be taken. The Company is responsible for ensuring that all Users strictly adhere to such requirements and prohibitions and is fully liable for any and all consequences arising from failure to comply with the requirement to safeguard the Identifiers, as aforesaid, including any noncompliance on the part of Users.**
- 5.3. It is not permitted to respond to e-mails that appear to be from the Bank and require Identifiers to be disclosed (for example by entering these on websites accessible via a link). The Bank must be informed immediately. Users must change their personal password immediately if there are grounds for suspecting that this has become known to another person.
- 5.4. The Bank reserves the right to define additional authentication methods (two or three level authentication systems). Accordingly, Users may be required to provide additional information to the Bank, for example a cell phone number for the purpose of sending text messages (SMS) or installing specific smartphone applications to authenticate Users using random one-time tokens.
- 5.5. Access to the Portal is provided through the public Internet. **Access to and use of the public Internet are the sole responsibility of the Company and the Users, and the Company and the Users shall assume all liability and risk in respect thereof, including in respect of any consequences arising from tampering and hacking by third parties where applicable.** The Bank cannot guarantee a connection, and is not responsible for providing a connection; neither can the Bank guarantee that Users will be able to connect to the Portal through the public Internet or any Internet service provider. The Bank shall provide its own website for the purpose of accessing the Portal and related services from the public Internet and the address of the website will be notified to the client separately.
- 5.6. On setting up the connection for the first time, Users will be required to change the password supplied by the Bank. The Bank is entitled to change the Identifiers at any time without notice, if such action is deemed to be necessary, for example for security reasons. In such circumstances, the Bank shall issue new Identifiers to the User without delay. Where there are grounds for suspecting that such Identifiers have become known to unauthorized third parties, the Company and the Users shall notify the Bank immediately to allow the codes to be replaced. The foregoing obligation specifically applies in the following circumstances:
  - Access to the services available on the Portal is barred.
  - There is reason to suspect that the Identifiers have been misused by unauthorized third parties.
  - Loss or theft of any or all of the Identifiers.

### 6. Risks and liability

- 6.1. There are inherent risks in using the Portal, such as the potential for information displayed on the Portal to be used for other purposes. The main risks involved are the following: (1) **Disclosure of the banking relationship and client information to third parties, which means that bank-client confidentiality can no longer be ensured;** (2) Changes to and falsification of information (for example impersonation and the provision of false information); (3) System failure and other communication disruptions which may cause delays, falsification, misrouting, or deletion of information; (4) Misuse resulting in loss or damage due to information being intercepted by third parties.
- 6.2. **Under the terms agreed with respect to authentication (compare clause 3), the User and/or the Company shall assume the risks associated with (i) tampering with computer systems by unauthorized parties, (ii) misuse of personal Identifiers, (iii) failure to exercise proper due diligence, or (iv) interference incidents during data transmission caused by unauthorized third parties.**
- 6.3. The Company and the User are also aware of the risks associated with sharing information and data across public and private networks, including the risk that the banking relationship and client information may be disclosed to third parties. Deliberate tampering or hacking into the User’s computer system by unauthorized parties cannot be ruled out, even if the data transmitted (with the exception of sender and recipient information) are automatically encrypted on accessing the Portal. **The risks of such incidents occurring are deemed to be under the control of the Company and/or the User, and are to be borne by the Company.** Until such time as any bar on access takes effect (see clause 6 below), the Company shall bear the risks associated with the use of personal Identifiers.
- 6.4. Unless otherwise required under applicable law, **the Bank expressly excludes all liability for any loss or damage, including direct, indirect and/or consequential loss, or any consequences whatsoever, which may be suffered by the Company and/or the User, any cardholder, and/or third party as a result of accessing and/or using the Portal, including unauthorized access or use.**
- 6.5. While the Bank has used all reasonable endeavors to ensure that the Portal is secure by taking such measures as are required and generally recognized and by deploying appropriate technical and security standards, total security cannot be guaranteed. The Company and the User are aware, in particular, that:
  - the workstations and computer systems of the Company and/or any designated User are not under the Bank’s control and may be subject to external attacks;
  - **there is the potential risk that unauthorized parties steal or intercept, and subsequently misuse, the Identifiers or other data of the Company and/or the User;**
  - information is sent over a public network and, although it is sent in the form of encrypted packets, it cannot be ruled out that information may pass through communication lines and nodes across national borders, notwithstanding that the sender and recipient are resident in Switzerland;
  - public network operators may be able to identify the Company, the User, and any

- counterparties with whom the Company or User may be in contact through the Internet;
- compliance with bank-client confidentiality requirements cannot be guaranteed under any circumstances, either with respect to the Portal or public networks.
- 6.6. In particular, the Bank takes no responsibility and accepts no liability for any loss or damage whatsoever that may be suffered by the Company, any designated User, and/or cardholder, (i) due to transmission errors, technical faults, system overload, disruption, damage, breakdowns, tampering or interception, (ii) due to unlawful interference with or hacking into telecommunications equipment or the blocking of telecommunications systems or networks, (iii) or due to other faults caused by system or network operators, while the Portal is being used. Neither is the Bank liable in general for any loss or damage that may be caused to the Company, Users, the cardholder, or third parties as a result of supplying data pertaining to the banking relationship over public networks.
- 7. Bar on access**
- 7.1. The Administrator may block access authorizations for other Users at any time.
- 7.2. The Company may submit a request to the Bank to block access authorizations for the Administrator or other Users at any time.
- 7.3. The Bank may bar Users from accessing the Portal at any time.
- 7.4. All Users may submit a request to the Bank for their access authorizations to be blocked. The Bank reserves the right not to comply with such request until it has consulted the Administrator.
- 8. Information on ATMs, terminals, computer screens or other IT systems**
- 8.1. While the Bank has used all reasonable endeavors and taken all reasonable steps to ensure the reliability, accuracy, and integrity of information and notices provided on the Portal, any data and documents supplied are intended for information purposes only.
- 8.2. The provision of such data and documents are not to be construed as implying any obligation or liability on the part of the Bank and may not be used by the client, designated Users, the cardholder, or third parties to institute claims, of whatever nature, against the Bank.
- 8.3. Information and notices displayed are deemed to be nonbinding and of a temporary nature only, unless specific information is expressly stated to be binding in relation to a particular service. Neither is such information to be construed as constituting a recommendation, offer, or solicitation to carry out transactions or enter into any legal transaction unless expressly stated as such.
- 9. Electronic agreements, electronic legal disclaimers**
- 9.1. The use of certain services provided through the Portal may be conditional upon agreeing to separate terms. The Bank may display such terms to the User in electronic form once the User has been authenticated through the Portal. The foregoing also applies to any variations or amendments to these Terms and Conditions.
- 9.2. The services will be activated once the User has successfully applied for the same, where necessary, and has agreed, electronically, to any additional special terms and conditions, whereupon the terms and conditions will become binding upon the User and the Company.
- 9.3. Agreements concluded electronically are deemed equivalent to agreements bearing a handwritten signature. The relevant terms and conditions may be printed out and viewed on the Portal. The Bank may change the range of services available at any time. Due to the globalization of markets and the continuing expansion of online services, the Bank is required to display additional legal notices in respect of information published and services available online. Such notices will become binding upon the User as soon as they are displayed. Users who are unwilling to acknowledge and accept such notices must also refrain from accessing the information/using the services.
- 10. Country-specific restrictions, foreign import and export restrictions**
- 10.1. The Company confirms that it is aware of and has informed Users that in accessing and using the Portal and/or related services outside Switzerland they may, in certain circumstances, be in breach of foreign laws and regulations. Accordingly, the Company shall (i) obtain information on the existence, contents, and scope of any legislation, regulations, and rules, in general, governing the use of banking services, which may apply in foreign countries from which it may access the Portal and related services; (ii) only use the Portal and related services insofar as such use is consistent with the aforementioned local provisions and regulations and, in particular, scrupulously comply with any bans and/or restrictions on the use of banking services; (iii) ensure that Users also comply with the aforementioned obligations.
- 10.2. The Company exempts the Bank from all liability in respect of the foregoing and accepts, irrevocably and without exception, full responsibility and liability in respect of any consequences, penalties, or breaches, that may arise as a consequence of using the Portal and related service outside Swiss territory.
- 10.3. The Company and the User also agree to indemnify the Bank from and against any direct or indirect loss or damage and/or consequential loss, charges, costs, and consequences, which may arise due to any breach of the aforementioned provisions or any other provisions of these Terms and Conditions governing use of the Portal or related services.
- 10.4. **The Bank is entitled to adjust or restrict the range of services available at any time without notice.** The Bank is not responsible for and is not liable in respect of any direct or indirect loss or damage or any consequential loss, which may be suffered by the Company or any User due to any bar on, suspension of, adjustment to, or interruption of access to any service or services, or to the Portal as a whole. The User is responsible for obtaining information on and complying with any relevant restrictions and legislation. The Bank accepts no liability in respect of such compliance.
- 11. Transmission errors, technical faults, outages, and unlawful interference**  
**The Bank accepts no liability** for any loss or damage caused by transmission errors, misrouting, technical faults and disruptions, outages, or unlawful interference in the computer systems of Users or third parties (including systems and networks that can be accessed by anyone), unless the Bank failed to exercise the standard of care customary in the industry. Insofar as the Bank has exercised the standard of care customary in the industry, the Bank makes no warranty that access to the services will be continuous, uninterrupted, or error-free. Neither is the Bank liable for any loss or damage due to malfunctions, outages (including systems maintenance), or overloading of the Bank's IT systems or ATMs.
- 12. Prices**
- 12.1. The prices charged for use of the Portal, the supply of related services, and the provision of Identifiers (including replacements and any additional Identifiers ordered) are set out in a separate price list.
- 12.2. Any adjustments to prices will be notified by suitable means. The prices stipulated will be charged to the Company immediately, monthly, quarterly, or on an annual basis at the option of the Bank.
- 13. Bank-client confidentiality/data protection, marketing**
- 13.1. Swiss law (for example governing bank-client confidentiality and data protection) solely applies within Swiss territory. As a result, any data transferred outside Switzerland will no longer be protected under Swiss law.
- 13.2. The Bank is entitled to store, process, and use any data pertaining to the Company or the User, which it may obtain in connection with their use of the Portal. More specifically, the Bank, or any third-party agents of the Bank, is permitted to analyze the aforementioned data, use data to create client profiles, and process data for marketing purposes. This will allow the Bank to provide personalized advisory services, provide customized offers, and keep clients informed of the Bank's products and services. The following data will typically be processed: information on the Company and Users and information on payment cards, and additional services.
- 13.3. The Company and the User may at any time opt out of receiving offers and information on the Bank's products and services. Any opt-out request must be submitted in writing to the Bank's customer services team. Any agents of the Bank and their employees are required to comply with Swiss data protection legislation.
- 14. Amendments**  
The Bank reserves the right at any time to amend these Terms and Conditions, any additional agreements, or special terms and conditions applying to individual services. Notice of such amendments will be given in writing, electronically on the computer screen (compare clause 8), by circular letter, or by other means and are deemed to have been approved unless an objection is raised in writing within 30 days of notification, but in any event upon the next occasion that the Identifiers are used.
- 15. Termination**
- 15.1. Either the Company or the Bank may, at any time, terminate use of the Portal to take effect for any or all of the Users.
- 15.2. **Notwithstanding termination, the Bank is entitled to process any orders initiated prior to the date on which termination takes effect, which is legally binding upon the Company.**
- 15.3. The Bank is entitled, at any time, to terminate individual services provided through the Portal with immediate effect without notifying the Company or the User.
- 16. Further provisions**  
These Terms and Conditions governing use of the Portal and related services complement and supplement all other terms and conditions governing the relationship between the Company and/or User and the Bank.
- 17. Applicable law and place of jurisdiction**
- 17.1. These Terms and Conditions governing use of the Portal and related services are governed by and construed in accordance with Swiss law.
- 17.2. **Lugano is the exclusive place of jurisdiction for any disputes that may arise between the parties with respect to the agreement set forth in these Terms and Conditions or the implementation and interpretation of the provisions hereof. The Bank is, however, also entitled to take legal action against the client in the court having jurisdiction in the client's place of residence or in any other court of competent jurisdiction. The foregoing is without prejudice to any mandatory places of jurisdiction prescribed under Swiss law.**

## 8. Company Signature(s)

Place/Date \_\_\_\_\_

Last name \_\_\_\_\_

First name \_\_\_\_\_

Signature\*  \_\_\_\_\_

\* Authorized signature(s) as recorded in the commercial register (individual or joint signature).

Company stamp 

Last name \_\_\_\_\_

First name \_\_\_\_\_

Signature\*  \_\_\_\_\_

Please complete, sign, and return the card application to: Cornèr Bank Ltd., Cornèrcard, Via Canova 16, 6901 Lugano