General Business Conditions for the Acceptance of Cashless Means of Payment

Version 07.2021 (CHE)

1 Scope of application and definitions

1.1 Scope of application

These General business conditions (hereinafter "GBC") shall apply with respect to the products and services agreed between the Merchant and Worldline Switzerland Ltd. (hereinafter "Worldline") in the modules for the acceptance of cashless means of payment, e.g. "Acceptance at the point of sale" or "Acceptance for secure e-commerce and mail/phone order" (hereinafter individually "Contract Module" or collectively "Contract Modules").

These GBC form an integral part of the Contract Modules concluded. The Contract Modules concluded form an integral part of the "Framework agreement for cashless payments" (hereinafter "Framework Agreement") concluded between the Merchant and Worldline.

1.2 Definitions

The following definitions correspond to the use of the respective terms in these GBC.

Acquirer (Worldline)	An acquirer enables its merchants to accept payment cards or other payment systems, e.g. **TWINT**, as a means of cashless payment within **presence** or **distance business** and ensures the processing of the **transactions** thus generated. To do so, it holds the authorization of the relevant **licensor.**
Alipay platform	Alipay.com Co Ltd. (hereinafter known as "Alipay") operates an international e-payment platform. The collaborative agreement established between Alipay and Worldline allows the Merchant to the accept cashless payments made by Alipay users.
Authorization	As part of the authorization process, the **card/TWINT issuer** verifies whether a **card/TWINT user app** is valid/ not blocked and whether the transaction amount is within the set limit.
Card issuer	Company authorized by the **licensor** for the issuing of **cards** to **cardholders.**
Card scheme	Licensor (such as Visa International, Mastercard International) for the issuance (issuing) and acceptance (acquiring) of **cards** and cashless means of payment.
Card verification code	Sequence of digits printed on a **credit card** (e.g. Visa [CVV2], Mastercard [CVC2]), which is used as an additional security feature in **distance business.**
Cardholder	Customer that purchases goods and/or services offered by the Merchant and pays for them on a cashless basis using a **card (transaction)**.

116.1302.02 CHE_EN/11.2021

Cards	Generic term for payment cards that are used to make cashless payments, i.e. **credit/debit cards.**
Chargeback	Reversal of a **transaction** delivered by the Merchant or of a reimbursement already credited as a result of a justified objection regarding the **transaction** by the **card**holder/ TWINT user or the respective issuer. The claim to reimbursement on the part of the Merchant lapses.
Contactless (contactless card, contactless reader, contactless transaction)	Execution of **transactions** using "near field communication" (NFC), an international standard for the transmission of data via radio technology. This requires a terminal with a contactless reader and a **card** with an NFC-compatible chip, e.g. a Visa with "PayWave" or Mastercard with "PayPass" functionality. The chip data is read by holding the **card** to the contactless reader.
Credit	Full or partial refund of a **transaction** to the **cardholder/ TWINT user** who was originally debited.
Credit card	**Card** used to pay for goods and services whereby the **cardholder** is debited subsequently (e.g. Visa, Mastercard, Diners Club/Discover, UnionPay, JCB).
Debit card	**Card** used to pay for goods and services whereby the account of the **cardholder** is debited immediately (e.g. V PAY, Maestro).
Distance business	**Transactions** where neither the **cardholder/TWINT user** nor the **card/TWINT user app** are physically present at the point of sale. In particular, these are carried out via the Internet, telephone, fax or letter.
Electronic execution	Execution and delivery of a **transaction** making use of a hardware or virtual **terminal** and the electronic delivery to the **system.**
EMV (EMV card, EMV chip, EMV terminal)	Specification for **cards** that are equipped with a processor chip as well as the associated chip card reader device (e.g. POS **terminals,** ticket machines, ATMs, fuel pump systems). EMV transactions are payments that are processed by having the card data read electronically at an EMV terminal from the processor chip of the **card**.
Infrastructure	The technical installations attributable to the Merchant for the acceptance of cashless means of payment by means of **electronic execution,** i.e. hardware or virtual **terminals** incl. peripheral devices such as cash registers and telecommunication equipment, routers, servers, etc.
Merchant Category Code (MCC)	Grid specified by the **licensors** that enables the Merchant's business activities to be allocated by the **acquirer** to one or more sector categories.
mPOS terminal	Mobile card reader that is operated by means of a compatible mobile end device (e.g. smartphone or tablet) and an app.
Payment confirmation	Electronic receipt generated by Worldline which is sent directly to the **TWINT user's TWINT user app** after each transaction.
Payment service provider (PSP)	A PSP offers payment solutions, e.g. an application (virtual **terminal**) that allows electronic means of payment to be accepted in a webshop.
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) is a **PCI standard** which aims to ensure companies implement security standards.
PCI standards	Security standards for the payment card industry defined by the Payment Card Industry Security Standards Council (PCI SSC) whose application is imposed by the **licensors.** More information can be found at pcisecuritystandards.org.
PIN (personal identification number)	Personal combination of digits that authenticates the **cardholder** as a legitimate user of a **card.**
Presence business	**Transactions** where both the **cardholder/TWINT user** and the **card/TWINT user app** are physically present at the point of sale.
QR code	2D barcode that is generated by the Merchant when executing the **transaction** and is read by the **TWINT user** by means of the **TWINT user app** and used to execute the payment.
System	The electronic authorization and settlement system operated by Worldline for processing **transactions.** The "myPortal" service pursuant to section 4.4 forms a part thereof.
Terminal (hardware or virtual terminal)	Hardware terminals are stationary or mobile devices used to execute **transactions.** Software components that allow hardware terminals to be connected to other peripheral devices (cash register systems, hotel reservation systems, fuel pump systems, etc.) are assigned to the hardware terminal. Virtual terminals are applications that allow **distance business** transactions to be executed. Software terminals are usually operated and sold by **payment service providers** (also Worldline).
Transaction	Cashless payment procedure within the framework of the card/TWINT acceptance carried out by the Merchant by means of **electronic execution,** with the transaction data subsequently being processed by the **system** of Worldline.
Transaction receipt	Physical or electronic confirmation of the execution of a **transaction** generated by a **terminal** or in the webshop.
TWINT	A system for cashless payments. It enables the Merchant to execute payments using mobile technology. Specifically, to execute a payment at a **terminal** or online, the **TWINT user** makes use of the **TWINT user app** on its smartphone.
TWINT issuer	Financial institution authorized by the TWINT licensor to issue the **TWINT user app.**
TWINT security features	Animated elements included in the electronic **payment confirmation** transmitted by Worldline to the **TWINT user.**
TWINT user	Participant registered with a financial institution who purchases goods and/or services offered by the Merchant and pays for them on a cashless basis using TWINT **(transaction).**
TWINT user app	The application made available to the **TWINT user** by the **TWINT issuer** for the purpose of executing payments using TWINT.

2 The Merchant

2.1 Identification of the Merchant

Worldline is obliged to identify the Merchant and its legal representatives and to record the business activities of the Merchant and correctly allocate them to the corresponding sector category (MCC). For this purpose, the Merchant shall provide Worldline with copies of the documents specified in the Framework Agreement as well as, on a case-by-case basis, with any further documents required.

2.2 Affiliation of points of sale and webshops

The Merchant's points of sale and webshops can be affiliated to the Framework Agreement at the time the contract is concluded. The subsequent affiliation of points of sale and webshops shall be agreed separately by the Contracting Parties.

2.3 Sector allocation (Merchant Category Code, MCC)

The Merchant operates in the sector categories specified in the Contract Modules and sells goods and/or provides services to cardholders/TWINT

users that are exclusively allocated to these sector categories. A separate contract module must be concluded for each sector category.

2.4 Changes on the part of the Merchant

Changes on the part of the Merchant (e.g. regarding its legal form, business activity, address, account details, legal representatives, points of sale or infrastructure) shall be immediately communicated by the Merchant to Worldline in writing. Worldline is entitled to invoice the Merchant for the expenses associated with changes.
In the event of a significant change in the ownership structure and control of the Merchant, the latter is obliged to inform Worldline in writing at least one month in advance. In such an instance, Worldline shall be entitled to request that the Merchant's identification, pursuant to section 2.1, be updated. Should higher risks arise therefrom, Worldline is entitled to terminate the Contract Modules with immediate effect. For as long as Worldline is not informed in writing of a legal succession, it may credit all reimbursements with discharging effect to the previous Merchant.
If the Merchant's credit rating deteriorates considerably (e.g. the opening of insolvency proceedings), the Merchant shall inform Worldline without delay. Worldline shall be entitled, at its equitable discretion, to immediately take suitable measures, such as adjusting reimbursement terms, withholding reimbursements or demanding appropriate collateral. The Merchant shall be notified without delay of the measures taken.
Worldline is entitled to, for the purpose of its risk management, assess the business activities (products and services) and the financial situation of the Merchant. The Merchant shall provide Worldline with the required information (including financial statements) within 10 days following Worldline's request.

3 Infrastructure of the Merchant

3.1 General

The Merchant shall be completely responsible for obtaining, operating and maintaining an infrastructure that is suitable for the electronic execution of cashless payments as well as for taking the technical security measures to prevent any misuse of the infrastructure; in particular compliance with PCI DSS pursuant to section 14.2. This shall also apply to changes to the infrastructure as a result of system adjustments on the part of Worldline in accordance with section 4.1, para. 3.
Only terminals (hardware and/or virtual terminals) that have been certified in accordance with the applicable PCI standard and the requirements set forth by the licensors may be used for the execution of cashless payments. EMV certification is a mandatory requirement for hardware terminals. Furthermore, certified terminals require approval, by one or more acquirers, in accordance with the country-specific requirements of the responsible body.
Manual processing of transactions is permitted only in exceptional cases, in particular in the context of the fallback procedures pursuant to section 10.

3.2 Obligations of the Merchant

3.2.1 General due diligence obligations

The Merchant is obliged to ensure through appropriate measures that no manipulation is possible, in particular no improper transactions, and that the terminals are protected against access by unauthorized third parties. The Merchant shall train its personnel in the correct handling and use of the infrastructure at adequate intervals, in particular upon its entry into operation. It shall also instruct its personnel about measures to be taken to prevent misuse and fraud.

3.2.2 Obligations regarding hardware terminals

The Merchant shall place all hardware terminals at the point of sale in such a way that the cardholder/TWINT user has direct access to the terminal (in particular the display, keypad and card reader) and cannot be observed in case a PIN entry is required.

3.2.3 Obligations regarding virtual terminals

The Merchant shall, with the appropriate level of care, protect the infrastructure used to operate virtual terminals, in particular the computers (including all related network components) and the data carriers (particularly card numbers, expiry dates or transaction data).

3.2.4 Information obligation/Right to information

At the request of Worldline, the Merchant shall provide information in writing on which terminals are in productive use. Furthermore, the Merchant authorizes Worldline to obtain this information directly from the terminal manufacturers/software providers or any other infrastructure suppliers. The Merchant shall provide assistance to Worldline in this respect.
The Merchant shall immediately notify Worldline in writing of any changes relating to hardware terminals or its webshop, in particular any shutdowns, replacements or changes of location/URL.

3.2.5 Transaction routing through third parties

The Merchant shall be entitled to enter into an agreement with PCI DSS-certified third parties (such as payment service providers, network operators) which deliver transactions to Worldline on behalf of the Merchant. Worldline shall not refuse acknowledgement of such third parties unless for reasons of good cause. Any costs arising in relation to connecting the third party, in particular for activation, fees, delays and faults, shall be borne by the Merchant. Worldline shall be entitled to invoice the Merchant for such costs and fees or to offset these against any reimbursements due for crediting to the Merchant.
The Merchant shall immediately notify Worldline in writing of any changes in relation to transaction routing via third parties or if it switches the third party used. Worldline shall be entitled to refuse such changes or such a switch of third party for good cause.

3.2.6 Acceptance through multiple acquirers

If the Merchant simultaneously procures acquiring services from more than one provider, it must be ensured at all times that the transaction data relating to each acquirer is kept separate. Working with third-party acquirers must in no way negatively impact the execution and security of the transactions to be processed by Worldline.

3.2.7 Use of product logos

The Merchant is obliged to clearly present the product logos received from Worldline. In addition, the Merchant is obliged to obtain written consent from Worldline for documents it has drawn up prior to printing or any publication (e.g. on the Internet) if these documents contain logos of Worldline or specifically mention Worldline.

4 Authorization and settlement system of Worldline

4.1 General

Worldline operates and supports the system in technical, organizational and administrative respects.
The Merchant shall have no right to the system being available at all times and operating without disruption. Worldline provides no warranty in this respect. Worldline shall be authorized to interrupt, at its equitable discretion, the operation of the system if it deems such an interruption to be necessary for imperative material reasons, for example system adjustments and updates, disruptions, risk of misuse.
Worldline reserves the right to make technical or organizational changes or additions to the system. If these entail modifications to the infrastructure, the Merchant shall implement these in accordance with the instructions from Worldline at its own cost. The Merchant is also obliged to accept the system adjustments and updates, in particular for the purpose of increasing security standards, carried out by Worldline and the system/infrastructure suppliers or terminal manufacturers.

4.2 Authorization

Unless otherwise expressly agreed, the Merchant is obliged to obtain authorization from Worldline for any form of acceptance by means of a procedure specified by Worldline. This does not apply to exceptions explicitly authorized by Worldline (e.g. contactless card acceptance by means of offline transactions).
The Merchant acknowledges that within the context of the authorization procedure, it can only be verified whether a card/TWINT user app is not blocked and no limit has been exceeded. An authorization granted therefore does not confer on the Merchant any claim to the reimbursement of the transaction by Worldline.

4.3 Transaction processing and settlement

The transactions delivered by the Merchant are processed and settled by the system. The resulting claims to reimbursement are credited to the Merchant and the bank of Worldline is instructed to remit the amount due to the Merchant's financial institution.

4.4 Web service "myPortal"

These general business conditions apply to the services offered by Worldline Switzerland Ltd. (hereinafter "Worldline") under the name of "myPortal". They comprise the electronic provision of reimbursement notices, transaction and terminal information, as well as reports and self-service functionalities, in connection with the acceptance of cashless means of payment.
The Merchant must specify vis-à-vis Worldline the individuals to be given access rights to the administration area of the myPortal platform. The personalized login credentials (hereinafter "login credentials") provided by Worldline entitle them to make changes to the services purchased and to the configuration on behalf of the Merchant.
The Merchant is responsible for ensuring that the login credentials are adequately protected against access by unauthorized third parties. Further-

more, the passwords shall be changed on a regular basis. Any party that identifies itself to Worldline using the login credentials, shall be considered as having been authorized by the Merchant to use the myPortal platform. Worldline only verifies the login credentials; no further authentication is carried out.
If there are grounds to suspect that unauthorized third parties have gained access to the login credentials, the Merchant must ask Worldline (contacts to be found at Worldline.com/merchant-services/contacts) immediately to block the login credentials. The Merchant shall be liable for any actions taken by third parties using the login credentials as it is for its own actions.
The Merchant can access the data stored on the myPortal platform for a period of at least 6 months. However, Worldline assumes no responsibility regarding the authenticity and immutability of data when downloaded, recorded or stored by the Merchant.

5 Acceptance

5.1 Obligations of the Merchant

5.1.1 General obligations

Irrespective of the amount involved, the Merchant is obliged to accept all cards of the agreed card brands and agreed card types (credit, debit or prepaid card) as well as TWINT as a means of payment for goods and/or services.
In all cases, within the context of the acceptance, the Merchant shall

- not split a transaction into different cards or into several instalments for the same card; unless
  - it concerns an initial payment paid in advance and a second payment as the final payment for a service or good that was rendered or delivered at a later date;
  - it concerns an instalment the term and individual instalment amount of which has been agreed in writing between the retailer and the card holder;
  - the card holder pays one part of the total amount by card and the remaining purchase amount in another form (e.g. cash or cheque).
- not split a payment across several transactions;
- not disadvantage the card/TWINT in comparison with other means of payment, in particular not request a surcharge for payment with the card/TWINT and not grant a discount to cardholders/TWINT users if they renounce payment with the card/TWINT in favor of other means of payment;
- not debit the card/TWINT in return for cash payments or loans granted; cash payments (Cash Advance, Purchase with Cash Back) require (where available) a supplemental agreement;
- only accept the card/TWINT for services that cannot be provided immediately if the cardholder/TWINT user receives written information (also by e-mail) that the service will be provided subsequently;
- not change/correct any data on a receipt after it has been signed; if a correction is required, a new receipt must be issued;
- take the measures expected of a diligent merchant to prevent the misuse of cards/TWINT and notify any suspicions of misuse to Worldline immediately.

5.1.2 Special obligations for Alipay acceptance

For the purposes of Alipay acceptance, the Merchant undertakes to deliver the following marketing data to Worldline:

- Merchant ID;
- Business category (food, shopping, services, other);
- Name, address and opening times of every point of sale;
- Description of points of sale.

These enable the Merchant to promote their business activities on the Alipay platform and are a requirement for Alipay acceptance.

5.2 Exclusion of acceptance

The Merchant may not accept the card/TWINT for

- transactions involving goods and/or services that are not offered or provided by the Merchant but by a third party (sub-acquiring prohibition);
- transactions that do not correspond to the agreed sector categories; an additional contract module must be concluded in order to execute transactions outside the sector categories specified in the Contract Modules;
- transactions that are illegal or immoral in its country, at the place of receipt and/or according to the law applicable to the legal transaction with the cardholder/TWINT user or that require an official authorization that the Merchant does not have;
- transactions attributable to the sectors adult entertainment (pornography, eroticism), tobacco, pharmaceuticals, gaming and gambling or auctions; transactions in these sector categories may only be executed based on a supplemental agreement;
- transactions used to load other means of payment (e.g. prepaid cards, gift cards or e-wallet solutions); the execution of these transactions requires a supplemental agreement.

5.3 Acceptance in presence business

In electronic execution by means of hardware terminals, the Merchant shall ensure that the reading of the card data and, where necessary, the entry of the PIN/the scanning of the QR code, can be carried out on the terminal by the cardholder/the TWINT user in person – without this being observed by the Merchant or third parties.
The following applies to card acceptance:
If the terminal does not request a PIN entry, the receipt generated by the terminal must in every case be signed personally by the cardholder on the signature line intended for this purpose. When using an mPOS terminal, the cardholder signs directly on the screen of the mobile end device. The following applies to UnionPay transactions: A PIN/six-digit combination of numbers is required for each transaction. In addition, each receipt must be signed by the cardholder. For contactless transactions, the applicable security standard is managed via the hardware terminal. If the security parameters saved on the card and/or hardware terminal allow, neither PIN entry nor signature are required. Otherwise, the cardholder is requested to enter the PIN or to sign the receipt generated by the terminal.
If the cardholder's signature is required for the card to be accepted, the Merchant may only accept the card if it

- is presented within the period of validity printed on it;
- is not a recognizable forgery;
- has all the relevant security features; and
- has been signed by the cardholder.

Furthermore, for transactions with signature confirmation, the Merchant shall ensure that

- the cardholder personally signs the receipt in its presence;
- the signature on the paper receipt/screen (for mPOS terminals) matches the signature on the reverse of the card; and
- the last four digits of the card number are identical to the last four digits of the number printed on the receipt.

In case of doubt, the Merchant shall check the identity of the cardholder against a piece of official ID (check that last and first names match) and note on the receipt that the data on the ID and on the card have been compared and verified. For mPOS terminals this note has to be recorded together with a reference to the corresponding transaction ID. For certain UnionPay cards, the name of the cardholder and expiry date are not shown on the card. In these cases, the Merchant has no obligation to carry out checks with respect to the period of validity of the card and the proof of identity of the cardholder.
If a cardholder has forgotten the PIN or the system does not allow any further PIN entries, the card may not be accepted in accordance with the fallback procedures described in sections 11.2 and 11.3.

5.4 Acceptance in distance business

5.4.1 General

For the execution of distance business transactions, the Merchant must always obtain the last name, first name and residential address of the cardholder/TWINT user as well as, in the event of card acceptance, the card number and expiry date of the card and validate the plausibility of this information; in particular if the delivery address and residential address differ. The Merchant must specify the company name used in the webshop or the app on all information transmitted to the cardholder/TWINT user (e.g. order, delivery and transaction confirmations, invoice).

5.4.2 Secure e-commerce in the webshop (3-D Secure procedure, card acceptance)

By authenticating the cardholder within the scope of "secure e-commerce" transactions, the Merchant can reduce the risk of fraudulent transactions subsequently disputed by the cardholder. For this purpose, a virtual terminal with merchant plug-in (hereinafter "MPI") is integrated into the Merchant's webshop. This virtual terminal can be obtained from Worldline or another payment service provider certified in accordance with PCI DSS. The MPI is required in order to execute transactions in accordance with the 3-D Secure standards of the licensor (e.g. "Verified by Visa", "Mastercard SecureCode" or "ProtectBuy"). During the transaction, the MPI establishes an encrypted connection with the server of the card issuer and verifies the password of the cardholder for secure e-commerce transactions, which allows the authentication and subsequent authorization of the transaction by the card issuer.
E-commerce transactions that take place without MPI (e.g. manual entry of card data on the virtual terminal) are only permitted in exceptional cases and are associated with a higher risk of charging back of reimbursements in accordance with section 10.

5.4.3 E-commerce in the webshop (TWINT acceptance)

To enable the transaction to be executed, a corresponding QR code is generated and displayed to the TWINT user as part of the checkout process.

The TWINT user scans the QR code and initiates electronic execution of the transaction. In cases where no QR code can be displayed and scanned, an alternative method is available in order to enable initiation of the payment using TWINT.
If TWINT is stored by the TWINT user as a means of payment for simplified payment (so-called User on File procedure (UoF)), the Merchant must ensure that he complies with the following obligations:

- the TWINT users in the Merchant's user account have the option of cancelling the existing TWINT registration and setting up a new one at any time;
- repeated transactions based on the setting up of a subscription are designated as such;
- when periodic UoF charges are applied that become payable at intervals of greater than 6 months, the TWINT users are informed about them at least 7 days prior to the due date in question;
- when a subscription is extended, the TWINT users are informed about the extension at the latest one week before the notice period expires;
- the implementation rules have been inspected at twint.ch/content/uploads/2020/12/EN.pdf, and followed;
- the credentials used to sign the transaction are handled in accordance with equivalent security standard as provided for in the PCI DSS regulations;
- the Merchant provides user account identifying information during the registration process;
- the PSP subcontracted by the Merchant or the Merchant himself generates the Merchant's private cryptographic key directly on a hardware security module (HSM) and encrypts the credentials with a cryptographic key through an additional private one held in the HSM;
- the PSP subcontracted by the Merchant verifies for each transaction that the certificate presented in these transactions to the scheme manager is from the legitimate Merchant (the legitimate Merchant is the Merchant for whom the certificate was issued).

Worldline may immediately chargeback to the Merchant all chargebacks of TWINT-UoF transactions received as a result of a complaint by the TWINT User or Issuer and offset them against the reimbursements to be paid out.

5.4.4 Distance business transactions by post, telephone or fax (mail/phone order)

Different rules apply to the acceptance of cards/TWINT through mail/phone order.
The following applies to card acceptance:
The acceptance requires use of a certified virtual terminal. The Merchant must destroy all manually recorded card data (in particular card number, expiry date and card verification number) after the transaction has been executed.
Mail/phone order transactions are executed without MPI and the 3-D Secure procedure. Therefore, the risk of charging back of reimbursements pursuant to section 10 is always higher.
The following applies to TWINT acceptance:
Mail/phone order transactions can be executed in two different ways:

- use of a certified virtual terminal;
- transmission of the QR code necessary for the transaction to the TWINT user by the Merchant.

5.5 Execution of credits

A credit may only be made with respect to a debit previously settled and the amount of the credit may not exceed the amount originally debited. The Merchant is not permitted to execute a refund in any other way than described hereinafter (e.g. in cash or via money transfer). Once the Merchant has executed a credit, Worldline is entitled to demand from the Merchant the repayment or offsetting of the transaction previously settled or reimbursed.
The following applies to card acceptance:
If a transaction is to be fully or partially refunded to the cardholder after it has been executed, the Merchant shall issue a credit to the same card.
With electronic execution, a credit transaction shall be initiated and a credit receipt printed out.
The following applies to TWINT acceptance and mPOS terminals:
If a transaction is to be fully or partially refunded after it has been executed, the Merchant is able to request a subsequent full/partial credit for a transaction from Worldline.
The following applies for Alipay acceptance:
Alipay allows credits to be handled which are within a period of 365 days. A credit can no longer be requested after this deadline ends. Using appropriate customer service provisions or with a suitable written notice, the Merchant must ensure that the user is notified of the 365-day deadline at the time of the transaction.

6 Receipts

6.1 General

Non-compliance with the obligations pursuant to sections 6.2 and 6.3 leads to a higher risk of charging back of reimbursements pursuant to section 10.

6.2 Transfer to the cardholder/TWINT user

In presence business, the original copy of the receipt printed out by the terminal is retained by the Merchant ("Merchant Receipt"). The Merchant hands over a copy ("Customer Receipt") to the cardholder/TWINT user.
When using an mPOS terminal, the receipt is transmitted to the cardholder via e-mail, if requested.
In distance business, the Merchant provides the cardholder/TWINT user with written confirmation of the transaction.

6.3 Safekeeping obligation

The Merchant is obliged to store all original paper receipts and copies of the electronic receipts, all transaction data and daily closing reports (incl. individual transaction data) as well as the related order data and documentation in a secure location for at least 36 months from the date of the transaction.
Electronic data must be stored in an encrypted form and be protected against unauthorized access. In this respect, the Merchant is obliged to comply with the relevant instructions issued by Worldline (pursuant to section 14.2).

7 Transaction delivery

7.1 Delivery deadlines

The Merchant is obliged to deliver the transactions to Worldline within 48 hours of their execution.
For transactions that arrive in the system of Worldline later than is stipulated in the aforementioned provision, Worldline reserves the right to deny the Merchant the claim to reimbursement or to reclaim/offset reimbursements previously credited.
In distance business (secure e-commerce, mail/phone order), the Merchant shall be obliged to deliver the transactions within 48 hours even if it is unable to send/deliver the goods in question immediately or provide the service immediately.
The Merchant bears the sole risk regarding the data transfer from the infrastructure of the Merchant to the system operated by Worldline, irrespective of whether this is carried out by the Merchant or a third party it has involved.

7.2 Delivery currency

The Merchant shall deliver the transactions in the currencies set out in the Contract Module.

7.3 Subsequent entry (card acceptance)

Provided the Merchant meets the delivery deadlines pursuant to section 7.1, it is possible to manually re-enter lost, incorrect or incompletely delivered transactions in cases attributable to a technical disruption to data transmission or processing. Incorrect bookings (e.g. amount booked is too high or too low) cannot be re-entered.
Transactions that are delivered after more than 60 days (debit cards) or 180 days (credit cards) cannot be re-entered. The same applies to transactions whose data is not entered into Worldline's system.

8 Reimbursement

8.1 The Merchant's claim to reimbursement

Worldline shall reimburse the Merchant in respect of the transactions delivered – after deducting the agreed fees and subject to a subsequent chargeback – at the agreed reimbursement frequency. The settlement details are shown on the reimbursement notice.
No payments are processed by Worldline on bank holidays. The Merchant accepts any delays to crediting resulting therefrom. Other country-specific or regional public holidays may result in additional delays.

8.2 Account for receiving reimbursements

The Merchant shall hold an account at a financial institution in the name of the company or the owner for the purpose of receiving the reimbursements. For proper processing, the IBAN and BIC of the corresponding account are required.
The Merchant acknowledges that if incorrect or insufficient account data is provided, transfers may either not be executed or may be made to another recipient. All costs and fees incurred for inquiries or any other related expenses shall be fully borne by the Merchant.
Worldline shall credit reimbursements resulting from the Contract Modules to the Merchant in the form of a collective payment. If the Merchant requests transfers for each card brand, it shall bear any additional costs arising in this respect.

8.3 Reimbursement currency
In principle, reimbursements are credited to the Merchant in the local currency valid at the Merchant's registered seat. If the Merchant requests crediting in another currency, the currency delivered by the Merchant is converted via CHF into the requested reimbursement currency. The foreign currency conversion rates specified by Worldline apply. The Merchant shall accept the conversion rates applied by Worldline.

8.4 Reimbursement notice
The reimbursement notice is provided by Worldline in the form agreed in the Contract Module. In every case, the reimbursement notice shall be made available in the web service "myPortal".
The Merchant shall notify Worldline in writing, within 30 days of provision within the web service or, in the case of other agreed forms of delivery, of receipt, of any objections in relation to the reimbursement notice; otherwise the reimbursement notice, including all the information contained in it, is deemed to be correct and complete and to have been approved without reservation.

9 Fees
9.1 General
All fees to be paid by the Merchant to Worldline are set out in the Contract Module. The fees shall fall due upon the service being provided by Worldline; they shall be offset against accrued reimbursements and listed on the reimbursement notice (section 8.1).
If the application of a schedule of fees is agreed in the Contract Module, the respectively valid version (available at Worldline.com/merchant-services/downloads) constitutes an integral part of the Contract Module.
The Merchant's claims vis-à-vis Worldline may only be offset with prior written approval of the latter. Worldline is entitled at any time to offset its claims vis-à-vis the Merchant.

9.2 Interchange fees
The Merchant may request information regarding the amount of interchange fees from Worldline in writing or access it via Worldline.com/merchant-services/interexchange.

9.3 Third-party crediting fees
The transfer fees or foreign currency crediting fees charged by the Merchant's financial institution, in connection with crediting shall be borne by the Merchant and be directly charged to the latter upon the reimbursement being credited. In the event of statutory changes and/or changes to fees charged by third parties, Worldline reserves the right to change its modalities of reimbursement.

9.4 Default of payment
If the offsetting of the amounts owed by the Merchant does not result in entire settlement thereof, Worldline will submit to the Merchant a request for payment for the outstanding amount. The term of payment is 10 days; upon its expiration the Merchant shall fall into arrears without further notice. In the event of the Merchant falling into arrears, Worldline shall be entitled to charge default interest at the rate of 10% p.a. on the outstanding amount and charge all costs for dunning and debt collection to the Merchant.

9.5 Taxes
The fees specified in the Contract Modules for products and services of Worldline are, unless otherwise specified, exclusive of VAT, withholding taxes and other duties. All taxes and duties which under the legislation of the Merchant's country are due or could in future become due with respect to the services to be rendered by Worldline within the scope of the Contract Modules shall be borne by the Merchant. In all cases, the Merchant is obliged to adhere to the provisions applicable in its country in relation to indirect taxes, withholding taxes and any other duties. The Merchant shall fully indemnify Worldline against any claims derived therefrom by third parties against Worldline.

10 Chargebacks and fraud monitoring
10.1 Chargebacks
The cardholder/TWINT user and the respective issuers are entitled to dispute a transaction provided that the prerequisites for the opening of a chargeback procedure, in particular the existence of a chargeback reason, are fulfilled.
In the event of a chargeback procedure being opened, the Merchant shall, following Worldline's request, submit to the latter, within 10 days and by registered mail, copies of all receipts and documentation (pursuant to section 6) suitable to refute the chargeback reason. If the chargeback reason cannot be refuted by means of the receipts submitted by the Merchant or if the receipts requested are not submitted in due time, Worldline is entitled to reclaim transactions already reimbursed or to offset them with reimbursements to be credited to the Merchant ("chargeback"). This also applies to cases in which goods and/or services are not directly delivered/ rendered by the Merchant but by third parties, particularly if the Merchant acts as intermediary or agent of such third parties.
If the Merchant, following the opening of a chargeback procedure, wishes to execute a credit in favor of the card/TWINT user app used in the disputed transaction, it shall inform the Chargeback department at Worldline about its intention. Following approval by Worldline, the Merchant shall execute the credit in accordance with the provisions set out in section 5.5. During the chargeback procedure, the Merchant shall refrain from taking any legal action against the cardholder/TWINT user.

10.2 Chargeback reasons in presence business (card acceptance)
With respect to card acceptance in presence business, Worldline shall, in particular, have a chargeback right if the cardholder disputes the transaction and the Merchant cannot prove that the card was present at the point of sale at the time of the transaction. This applies, in particular, if the Merchant
- upon accepting EMV cards, reads the card data via a "non-EMV terminal" (without EMV chip reader); or
- does not read the card data from an EMV chip or magnetic stripe, but enters it manually via the keypad of the terminal (in accordance with the fallback procedures pursuant to sections 11.2 and 11.3.);
- upon accepting cards, uses an imprinter and the receipt is not signed by the cardholder.

This list of chargeback reasons is not exhaustive.

10.3 Chargeback reasons in distance business
With respect to acceptance in distance business, in particular, the following chargeback reasons apply:
- the cardholder/TWINT user disputes the order and/or receipt of goods or services;
- the cardholder/TWINT user rejects the goods received as defective or as not being those specified in the order;
- the cardholder/TWINT user withdraws from a purchase of goods and/or services within the statutory withdrawal period;
- the cardholder/TWINT user asserts claims vis-à-vis the Merchant or for any other reason refuses to fulfill the claim resulting from the transaction;
- a card transaction was executed without 3-D Secure procedure.

This list of chargeback reasons is not exhaustive.

10.4 Fraud monitoring
Within the context of fraud monitoring, Worldline is entitled at any time to issue instructions to the Merchant aimed at preventing fraud cases (e.g. obligation for cardholders to provide ID). These instructions come into force as soon as the Merchant has been notified thereof and the Merchant is obliged to fully comply with them.
In the event of reasonable suspicions of fraud, Worldline is entitled to withhold the reimbursements to the Merchant until the suspicions have been clarified. This remains subject to sections 10.2 and 10.3. In the event of an excessive number of fraud cases, Worldline also reserves the right to terminate the Contract Modules with immediate effect.

10.5 Compliance with the limits
Each month the Merchant shall ensure that for the card brands agreed/ TWINT the following thresholds are kept:
- ratio of the total volume of chargebacks plus credits/to gross sales per month shall not exceed 2%;
- ratio of the number of chargebacks plus credits/to the number of transactions per month shall not exceed 1%;
- ratio of the total volume of fraudulent transactions/to gross sales per month shall not exceed 0,75%;
- ratio of the number of fraudulent transactions/ to the number of transactions per month shall not exceed 3% and less than 3 fraudulent transactions.

If either of these thresholds is exceeded, Worldline is entitled to charge the Merchant case-specific expenses for each chargeback/credit/fraudulent transaction in excess of these limits. Furthermore, Worldline is entitled to pass on any penalty and/or processing fees imposed by the licensors to the Merchant, to defer the reimbursement of the transactions delivered for up to 180 days and to terminate the Contract Modules with immediate effect.

11 Functional disruptions and fallback procedures
11.1 General
The following functional disruptions may occur:
- functional disruption to the system;
- functional disruption to the infrastructure or the terminal;
- functional disruption to the card (damaged card) or the TWINT user app.

The following applies to card acceptance:
In the event of functional disruptions, the Merchant may use the manual fallback procedures pursuant to sections 11.2 and 11.3. Alternatively, manual

processing by means of an imprinter can be used. In doing this, the Merchant must adhere strictly to the data sheet „Manual settlement using an imprinter". The Merchant acknowledges that for transactions executed using the fallback procedures, there is a higher risk of charging back of reimbursements pursuant to section 10.
When applying the fallback procedures, the Merchant shall in each case request from the cardholder a piece of official ID and match the data on the ID (last name and first name) against that on the card. After completing the fallback procedures, the Merchant is obliged to immediately destroy all manually recorded card data. Under no circumstances may the Merchant file or store the card verification number or any data read and saved from the magnetic stripes of cards after the transaction has been authorized.
There is no fallback procedure for transactions with Visa Electron, V PAY, Maestro and UnionPay as well as for Dynamic Currency Conversion (DCC) transactions.
The following applies to TWINT acceptance:
In the event of a functional disruption no transactions can be executed.

11.2 Fallback procedures for functional disruptions to the system/ terminal (card acceptance)

If the system or the terminal of the Merchant fully or partially fails, the Merchant shall authorize each transaction with Worldline by telephone until system operation is resumed/the terminal is functioning again. Once system operation has been resumed, the transaction data as well as the authorization number obtained shall be entered manually by the Merchant on the terminal using the "Booking authorized by telephone" function.
In the event of a functional disruption on the mPOS terminal, there is no fallback procedure available.

11.3 Fallback procedures for functional disruptions to the card (card acceptance)

If the functional disruption is a result of damage to the card, the Merchant may manually enter the card data on the terminal. The Merchant shall authorize such transactions in advance with Worldline by telephone. The manual entry of data by typing in the card data on the terminal must be executed using the "Manual card data entry" function. The receipt printed out by the terminal must be signed personally by the cardholder.

12 Additional provisions for hotel or car rental reservations (card acceptance)

With respect to the acceptance of credit cards for hotel or car rental reservations, the Merchant shall additionally adhere to the provisions on the respectively applicable data sheet, "Hotel reservation guarantee per credit card"/"Hotel reservation by means of down payment with a credit card (Hotel Advance Deposit)"/"Rental car reservation with a credit card". The respective data sheet forms an integral component of the Contract Module.

13 Additional provisions for Dynamic Currency Conversion (card acceptance)

The dynamic currency conversion (DCC) service allows dynamic currency conversion at the terminal. An overview of the foreign currencies available can be requested from Worldline.
The Merchant shall ensure that the cardholder can in all cases independently select whether he/she wishes to carry out the transaction in the card currency (DCC transaction) or in the local currency.
For DCC transactions, the foreign currency conversion rate (local currency/ card currency) specified by Worldline for the accepted foreign card shall apply to the cardholder. The Merchant shall accept the conversion rate specified by Worldline.
Worldline shall be authorized, at its equitable discretion, to interrupt the operation of the DCC service or of individual foreign currencies if it deems such an interruption to be necessary for imperative material reasons, for example disruptions, risk of misuse or extraordinary volatility on the foreign exchange markets.

14 Data protection

14.1 Processing of personal data

Worldline, as data controller, processes personal data in accordance with the applicable legislation. The processing of personal data is further elaborated in Worldline's Privacy Notice (worldline.com/merchant-services/data-privacy).

14.2 PCI DSS data security standard

Card data (in particular card numbers, expiry dates) shall be protected against loss and unauthorized access by third parties. The licensors' data security provisions that must be met to this effect are defined in the PCI DSS. In this respect, the Merchant shall observe and at all times fully comply with the currently applicable version of the "PCI DSS compliance instructions security standards" issued by Worldline, which forms an integral part of these GBC. In particular, the Merchant is obliged to carry out the certification measures, e.g. self-assessment questionnaire, and confirm to Worldline its compliance with the PCI DSS.
In the event of card data being stolen or if it is suspected that card data has been stolen, the Merchant shall notify Worldline immediately. In such a case, the Merchant expressly authorizes Worldline to mandate an audit company accredited by the licensors to produce a "PCI audit report". This will involve investigating the circumstances in which the damage arose and verifying whether the Merchant complied with the PCI DSS. The Merchant is obliged to cooperate fully with the audit company; in particular, it shall provide the audit company with unrestricted access to its premises and infrastructure. After the PCI audit report has been produced, the Merchant shall, at its own expense, completely resolve all the security defects identified within a period of time notified by Worldline. If the investigation reveals that the security standards in accordance with PCI DSS were not met at the time the data was stolen, the costs incurred in producing the PCI audit report shall also be borne by the Merchant.
Worldline shall be entitled to pass on any claims for damages put forward by the licensors to the Merchant and/or to terminate the Contract Module with immediate effect if the Merchant does not comply with the PCI DSS or if the Merchant does not confirm, upon request, that it is complying with the PCI DSS. This shall apply equally in the event of card data being stolen or if it is suspected that card data has been stolen.

15 Liability

Notwithstanding ancillary statutory provisions and unless explicitly regulated otherwise, the Merchant shall be liable, in particular, for damage that Worldline incurs as a result of the former, or third parties involved by it, failing to fulfill their obligations, notably in technical, organizational and administrative respects. In particular, Worldline is entitled to pass on to the Merchant any potential claims for damages resulting from a culpable breach of duty by the Merchant or by third parties involved by it as well as any penalty and/ or processing fees imposed by the licensors and any other case-related expenses. The Merchant shall fully indemnify Worldline in this respect and shall be liable for these claims and any additional case-related expenses.
Unless explicitly regulated otherwise, Worldline or third parties involved by it shall be liable in case of wilful misconduct or gross negligence in accordance with the statutory provisions. The liability of Worldline for slight negligence shall be fully excluded.
The liability of the Contracting Parties for culpable harm to life, body or health as well as the statutory product liability remain intact.

16 Notifications

All notifications shall be issued in writing unless another form has been explicitly agreed in the Contract Module. Written form also includes electronically transmitted messages (e.g. via e-mail or via a platform provided by Worldline within the scope of a service).

17 Modifications and additions to the Contract Modules, incl. fees

Modifications and additions to the Contract Modules, in particular the GBC and other integral parts, must be made in writing in order to take effect.
Worldline reserves the right at any time to modify or make additions to the Contract Modules, in particular the GBC and other integral parts as well as the fees. These modifications or additions shall be communicated in writing to the Merchant at least 30 days prior to their coming into force. If the Merchant does not communicate its refusal of the announced modifications or additions in writing and before the proposed effective date of the modifications or additions, this shall be deemed to represent acceptance of the modifications or additions. Excluded are modifications of the schedule of fees; the respectively applicable version is published at Worldline.com/merchant-services/downloads and comes into effect upon its publication.
Taking security measures in accordance with section 2.4, para. 3, making changes to the system in accordance with section 4.1, para. 3 as well as modifying the fees within an agreed charging framework are not deemed to be modifications within the meaning of this section and therefore do not represent grounds for termination.

18 Coming into force, duration and termination

18.1 Coming into force

In principle, the Contract Module comes into force once Worldline has sent the activation confirmation to the Merchant. If, however, the Contract Module explicitly foresees countersignature by Worldline, the Contract Module shall come into force upon being signed by the Contracting Parties.

18.2 Duration

The Contract Module is concluded for an indefinite duration, leastwise for any minimum contract duration agreed upon. Once the minimum contract

duration has elapsed, the Contract Module shall automatically be extended for recurrent periods of 12 months, provided it has not been terminated by one of the Contracting Parties.
The Merchant's right to termination pursuant to section 17 and the right to immediate termination for good cause of the Contracting Parties, pursuant to section 18.4, remain reserved.

18.3 Ordinary termination
Unless otherwise agreed, the Contract Module may be terminated subject to 6 months' notice by registered mail, for the first time as per the end of the minimum contract duration, then as per the recurring date 12 months after the end of the minimum contract duration. If there is no minimum contract duration, the termination date is the annually recurring date on which the Merchant signed the Contract Module.
Notification of termination of one Contract Module does not cause the termination of the remaining Contract Modules. If no further Contract Modules exist, the termination of the last/sole Contract Module automatically results in the dissolution of the Framework Agreement.

18.4 Extraordinary termination
In the event of good cause, the Contracting Parties shall be entitled at any time to terminate the Contract Modules with immediate effect. In particular, good cause includes the following:
- serious or repeated breaches of the provisions of the Contract Module by either Contracting Party;
- repeated complaints/chargebacks and/or transactions being reported by card/TWINT issuers as fraudulent (pursuant to section 10);
- other inconsistencies in settled transactions;
- a significant change in the ownership structure and control of the Merchant;
- the opening of insolvency proceedings over the assets of the Merchant.

The extraordinary termination of Contract Modules for the acceptance of cashless means of payment authorizes Worldline to immediately terminate all existing contract modules. The immediate termination of all existing contract modules causes the Framework Agreement to be automatically rescinded.

18.5 Automatic termination
The Contract Modules shall automatically terminate, without requirement of notice, if for a period of 2 years no transaction deliveries by the Merchant have occurred.
The automatic termination of Contract Modules for the acceptance of cashless means of payment results in the automatic termination of all existing contract modules as well as the Framework Agreement.

18.6 Consequences of contract termination
The obligations arising out of sections 6.3 (Safekeeping obligation), 14 (Data protection), 15 (Liability), 18.6 (Consequences of contract termination), 19 (Confidentiality), 20.3 (Assignment prohibition) and 20.7 (Applicable law and place of jurisdiction) shall remain in place following termination of a Contract Module.
Following termination of the Contract Module, the Merchant shall remove all references to the corresponding services of Worldline visible to customers.
Upon notice of termination of a Contract Module, Worldline is entitled to withhold the crediting of reimbursements to the Merchant immediately and for 180 days beyond the termination date of the Contract Module in order to offset any subsequent claims, in particular chargebacks, against these reimbursements.
If criminal or any other legal proceedings are opened against the Merchant or charges have been brought against the Merchant, Worldline reserves the right to delay the crediting of reimbursements at least until the proceedings have been completed.

19 Confidentiality
The Contracting Parties reciprocally undertake to keep confidential the agreed commercial conditions as well as all information, documentation, data and processing techniques – described or identifiable as being confidential and neither publicly nor generally accessible – that they become aware of in fulfilling the Contract Modules; they may only make these accessible to third parties with prior written consent from the other Contracting Party. This does not prevent any Contracting Party from disclosing confidential information insofar as it constitutes a performance of mandatory provisions of law.

20 Concluding provisions
20.1 Right to issue instructions of Worldline
The Merchant is obliged to comply with the technical, organizational and administrative instructions and guidelines issued by Worldline as well as the terminal and infrastructure suppliers.

20.2 Intermediary activities of Worldline
Worldline also acts as an intermediary for other acquirers and infrastructure suppliers and in doing so, brokers their contracts in their name, at their risk and on their account. The contracting parties for services provided in this manner are the respective service provider and the Merchant.

20.3 Assignment prohibition
The Merchant may only assign any of the rights or duties it has vis-à-vis Worldline with prior written consent from Worldline.

20.4 Involvement of third parties/assignment to Group companies
Worldline reserves the right to transfer the fulfillment of its contractual obligations to third parties at any time, without having to inform the Merchant.
Worldline is entitled to assign the Contract Module to another Group company. In such a case, the Merchant is to be suitably notified.

20.5 Waiver of rights
If any rights arising from the Contract Modules are not asserted by Worldline, this in no way represents a waiver of these rights unless Worldline has issued an express written waiver declaration in this regard.

20.6 Severability clause
Should a provision of the Contract Modules (including fees) be declared invalid, the remaining provisions shall not be affected thereby and are to be construed in such a way as if the Contract Module concerned was concluded without the invalid provision. The same applies to any contractual omissions.

20.7 Applicable law and place of jurisdiction
All legal relationships between the Merchant and Worldline arising from the Framework Agreement and from all Contract Modules concluded are subject to Swiss law. The exclusive place of jurisdiction is Zurich.