Combo payment methods

Fallback procedure if payment terminal malfunctions

Card data may generally only be read into the payment terminal from the chip, magnetic strip or NFC. The contractual partner may not accept the card without the presence of the cardholder who must present the card. When processing manual transactions using the fallback procedure, the contractual partner is obliged to follow the procedure below.

Risks associated with processing manual transactions
The contractual partner acknowledges that there are risks associated with the processing of transactions in this way and that they must bear these risks. In such cases, the contractual partner bears the full risk of collecting the transaction amount from the cardholder.

Procedure in the event of disruptions due to problems with the terminal

In the event of total or partial failure of the contractual partner's system or terminal, the contractual partner may resort to the manual fallback procedure (if available) until the system is operational or the terminal is functioning again.

The fallback procedure can be used with the following payment methods: Visa, Visa Debit, Mastercard®, Debit Mastercard and Diners. There is no fallback procedure if other payment methods used fail or an mPOS terminal fails.

In any case, always ask for the cardholder's official ID and check that the ID details (last name and first name) match those on the card. If the details match, make a copy of the ID card. The copy remains with the contractual partner and must be provided to PostFinance on request.

↓

Each transaction must be authorized by telephone through Worldline's authorization center (open 24 hours a day). Call +41 848 83 2000 and follow the instructions:
1. IVR selection: language (1 – DE / 2 – FR / 3 – IT / 4 – EN)
2. IVR selection: press 2 for "Authorization"
3. IVR selection: press 1 for "Authorization"
4. IVR selection: press 2 for "Authorization"
5. IVR selection: enter your nine-digit contract number
6. IVR selection: now enter the card number
7. IVR selection: etc.

↓

Make a note of the authorization number you received from the authorization center.

↓

Once the system is operational again, the contractual partner must enter the transaction data and the authorization number received manually on the terminal using the "Transaction authorized by telephone" function or, alternatively, notify PostFinance using the "Manual transaction entry" form.

↓

Destroy all manually recorded transaction data. Under no circumstances may the stored data be kept longer than after the transaction has been authorized.

Complying with the PCI-DSS guidelines
If you have to retain card data on-site, you should ideally use physical storage. In the case of electronic storage, comprehensive PCI-DSS certification is required to ensure the security of the card data. See our "Directives for compliance with the PCI-DSS security regulations for contractual partners". Keep the card data stored on paper (card number and expiry date) in a safe place that is accessible only to a limited and authorized group of people. Ensure that the card data is deleted or destroyed after the transaction has been authorized. Do not query or store card verification codes (CVV2, CVC2, CID, CAV2).

VISA VISA DEBIT debit Diners Club INTERNATIONAL

PostFinance Ltd
Mingerstrasse 20
3030 Bern
Switzerland

www.postfinance.ch

460.373 en (dok.pf/pf.ch) 02.2025