

Chargebacks, Refunds and Cancellation policy, Complaints and Disputes Resolution Policy

Version 1.0.

Valid from 16/04/2024

1. General Covenants

Kaurifinance OÜ (hereinafter “the Company”) is a legal entity, registered and regulated by the laws of Estonia.

The purpose of this Chargebacks, Refunds and Cancellation policy, Complaints and Disputes Resolution Policy (hereinafter “the Policy”) is to ensure that the Company has internal guidelines to provide the maximum possible effective customer service and positive customer experience, therefore any customers' questions and concerns regarding their Transaction activity is being thoroughly investigated and properly addressed.

The User has a right to a Transaction chargeback / refund / cancellation only under specific conditions. In general, any Transaction initiated by the User is final and cannot be refunded.

This Policy is also applied to all Transactions made to/in/from the Company’s platform.

Since deposits have been utilized as a highly-demanded financial instrument all around the world, the Company has faced the increased number of victims of the card payment fraud and forgery schemes (e.g. Ponzi scheme, pyramid schemes, social engineering). In general, the Company can identify such cases only after personal complaints from an affected individual because they create accounts, top up wallets and transfer money to scammers by their own will. However there are also other means of fraudulent Transactions to be identified when the fraudster uses the victim’s card without the victim’s knowledge or permission.

As a merchant and a VASP the Company should prevent and act properly in any cases of fraud to avoid financial and reputation risks in accordance with a risk-based approach.

The Company’s Transaction Monitoring team has identified the steps necessary to address such situations and developed the current procedure in order to deal with disputable Transactions in the proper manner in the interest of our company as well as Users' security.

A dispute is a situation in which a person questions the validity of the initiated Transaction. A dispute occurs when the User contacts their card issuing bank and claims to have their money returned.

Disputes may arise for a number of reasons.

Standard dispute reasons usually include (inter alia):

- A) the User claims he has never initiated such Transactions;
- B) the User claims that the Transaction was not initiated or authorized (e.g. the card information was stolen and used fraudulently);
- C) an error, such as duplicate billing, - incorrect amount billed, or a refund was promised but never received;
- D) the User claims about the scam by an unauthorized entity.

2. Cards Chargeback

In case of card deposits the Company accepts deposits only from cards that support 3D-Secure functionality and the User accepts this.

Meanwhile, as in every case of Card-Not-Present Transactions, the merchant carries a higher level of dispute risk. This is due to the situation where there is not always a possibility to provide traditionally accepted evidence to show that the actual (true) User authorized and/or participated in the Transaction.

A retrieval request, also known as a “soft” chargeback, takes place when the card issuer contacts the merchant (the Company) to obtain information about a Transaction charged to one of its Users.

The reasons for retrievals can be inter alia:

- A) it may be a result of a customer question or dispute, inaccurate or incomplete Transaction information,
- B) a processing error or an indication of potential fraud,
- C) the bank will request a legible copy of the Transaction authorization proof.

The User may initiate retrieval when they do not recognize the Transaction or may ask for specific information regarding the Transaction.

If a User opts to dispute a Transaction for the second time, or a card issuer finds the documents provided by us insufficient, the Company may receive a pre-arbitration / 2nd chargeback notice.

Pre-arbitration refers to the part of the chargeback process when the card issuer, or the User, disputes our representation and sends the case to the card network for a final decision in arbitration. This can only happen after the Company has won the first chargeback and there has been the third round of contestation for a disputed charge, a formal procedure to clarify whose claim has standing. An issuer's or User's comment (message) is often provided to us at this stage.

The Company's Transactions Monitoring team then edits the initial dispute response in accordance with the new information received; some additional data and documents may also be provided if needed.

The last one and the most important level of dispute is arbitration which allows merchants and Users to take a final stand and claim the resolution, whether it is a chargeback or a chargeback reversal, should be overturned. The arbitration procedure may only start if the Company wins a second chargeback, but a plaintiff (e.g. customer or his/her solicitor) is still unsatisfied. To resolve a dispute the card network (Visa or Mastercard) will be a judge between the plaintiff and a defender.

A pre-compliance chargeback is issued after the Company has successfully disputed a chargeback, but the issuing bank disagrees with the outcome. The bank might insist a card network rule was violated, meaning there was a compliance issue. The processor accepts a pre-compliance chargeback; the act essentially turns the previous representation win into a loss. (This exception doesn't affect the chargeback-to-transaction ratio: the damage is being done with the original chargeback that was filed and isn't being assessed a second time).

Our response to the pre-compliance cases are similar to the pre-arbitration: Transactions Monitoring team updates the initial dispute response and provides additional documents and information to clarify the situation.

Disputes processing include (inter alia):

- A) the User queries the Transaction;
- B) the Issuer files a report and notifies the Company's processing partner about the Transaction;
- C) the Processing partner notifies the Company about the dispute and blocks the Transaction amount in their business panel;
- D) the Transactions Monitoring team identifies the account operated by the Account to which the disputed card deposit had been made. Since most disputes the Company believes start to receive are connected to instances of fraud, this account may be temporarily suspended.
- E) the Transactions Monitoring team creates a task in the Transaction Monitoring space and prepares a response for the processing partner.
- F) the Company Transactions Monitoring team provides explanation and evidence to the processing partner's dispute officer.

Prepared response contains (inter alia):

- A) Description of the services provided. Most Transactions the Company predicts will be disputed are in fact fraudulent, made either with stolen cards or through defrauding, such as social engineering the User into paying for services they are never going to receive. So

the response to the dispute contains not only the description of the services the Company provides and documents confirming the successful Transaction, but also as much proof as the Company can provide that the User had fallen victim to fraudsters' false claims which the Company has nothing to do with;

- B) Description of our means of the client identification, KYC and AML profile of the client;
- C) Description of our communication with the client/User (if any);
- D) Proof of the top-up/deposit (extract from the Company's system);
- E) Proof of deposit delivery (extract from the Company's system);
- F) Withdrawal details if any (extract from the Company's system).

If possible, the response document is then converted to .pdf format and sent to the processing partner via email.

Processing partner confirms that they have received the Company's response documents and their sufficiency.

If the dispute is accepted (the Company chooses to refund the disputed amount), the Transactions Monitoring team notifies the processing partner about the decision, and the amount is credited from the Company's merchant account.

This can happen if the disputed Transaction is a result of a technical error (double charge).

If after choosing to challenge the dispute and provide the requested information to processing partner the Company does not receive any further response re the case, the case is considered won.

The Company may receive a formal notice from the processing partner that the User has not come back and the disputed funds are to be released.

If the User wishes to continue disputing the Transaction, or the card issuer finds the documents provided by us insufficient, the Company may receive pre-arbitration and pre-compliance notices. An issuer's or User's comment is usually provided at this stage.

The Company's Transaction Monitoring Team edits the response in accordance with the new information received; some additional data and documents may also be provided if needed.

If the pre-arbitration or pre-compliance is won, the Company receives a notice from the processing partner via email and closes the case.

3. Exchange Transaction Refund

A refund for the Exchange Transaction can be requested only in such cases:

- A) if an incorrect Exchange Transaction occurs as a result of the Company's failure, or
- B) if the User deposited the Funds to the Platform and no further Exchange Transaction was initiated, which means that the Funds in return for the User's Deposit were not sent to the User's designated digital wallet address or bank account within the usual time frame for the Exchange Transaction execution.

Refunds for the Exchange Transactions, at the Company's sole discretion, will be processed in the same currency as the initial deposit placed to initiate the Transaction.

4. Wallet Transaction Refunds

Refunds for the Wallet Transactions can be requested only if an incorrect Wallet Transaction occurs as a result of our failure. Refunds for the Wallet Transactions are provided in the same currency as the refunded Transaction.

5. Non-refundable Transactions

Refunds are not available in the following cases:

- A) the Transaction has already been duly initiated, and the Funds have already been sent to the designated bank account or digital wallet address;
- B) virtual currency of one type have been sent to a digital wallet intended for a different type of virtual currency (cross-chain deposits);
- C) the digital wallet address or bank account details provided by the User are incorrect;
- D) the Transaction has been initiated by indicating the digital wallet address or Blockchain network not supporting the particular type of virtual currency chosen by You;
- E) the User has no control or access to the digital wallet address or bank account indicated to perform the Transaction;
- F) the User has mistakenly indicated the Transaction amount or any other Transaction details;
- G) the Transaction has been initiated due to a security breach on the Your device/Account, or as a result of unauthorized access to Your Account;
- H) anonymous payment methods have been used;
- I) the name of the User differs from the name on the payer's bank account;
- J) the User has misrepresented or coerced into performing a Transaction by a third party;
- K) the Transaction has been initiated in breach of the Platform's rules and procedures;
- L) the access to the User's account has been lost due to the User's negligence.

This Policy is subject to change according to the ongoing situation on the market and in case of change / increase of fraudulent activity within the Company.

If there are any questions regarding this Policy You may contact our Support Team at support@kauri.finance