



**Payments & Withdrawals Policy**  
**Ver. 01\_5/2018**

## **1 Introduction**

**Blackridge Capital Management Ltd.** (hereinafter referred to as “**Blackridge**”, “**we**”, “**us**” or “**the Company**”) is committed to preventing, detecting and not facilitating money laundering and terrorism financing activities. The Company also aims to comply with anti-money laundering (“**AML**”) and counter-terrorism financing (“**CTF**”) recommendations in a way that complements business priorities

Due to the international nature of payments and withdrawals to and from Customers the Company is required to have robust systems and controls in place to prevent the risk of money laundering (“**ML**”) and terrorist financing (“**TF**”), which the business could be exposed to. As a result of these internal systems and controls the Company’s its overall Financial Crime Framework and risk management framework is strengthened.

This policy outlines the process of taking the instructions from a Customer, through to the transference of funds back to the Customer, as well as how to deal with issues that can occur throughout the process.

Blackridge Capital Management Ltd. has an in-house back office department responsible for processing Customer deposits and withdrawal transaction requests.

This policy and procedures contains important information on how to deal with identified third party payments, deposit and withdrawal procedures, the checks must be conducted by the relevant teams before a withdrawal or deposit can be processed. Further, red flags are highlighted in order for all relevant employees to be aware of when dealing with Customers.

This policy along with the Anti-Money Laundering and Counter Terrorist Financing Policy and Accounts Opening Procedure form the Company’s Anti- Money Laundering and Counter Terrorist Financing Manual (‘the AML Manual’).

## **2 Payment Methods**

### **2.1 Acceptable payment methods:**

The Company accepts the following payment methods:

1. Credit/Debit Card
2. BACS/Telegraphic Transfer/SWIFT (“Bank Transfer”)
3. E-wallets

Generally, one or more of the above payment methods are always available to Customers.

### **2.2 Not acceptable payment methods:**

There are a number of methods that are **not available** for Customers to fund their accounts:

1. Cash payments
2. Bank drafts

3. Bank cheques
4. Third party payments

### ***3 General information about payments***

- 3.1 **Receipt of Payments:** once a payment is received it is matched to a Customer and allocated by a member of the back-office payments team.
- 3.1 **Base Currency:** all Customers pay and withdraw funds in their nominated base currency of Euro (EUR), US Dollars (USD) and UK Pounds Sterling (GBP).
- 3.2 **Source of deposit and/or funds:** Customers acknowledge that they may be required to provide information on the source(s) of the deposit(s) and/or the Customers' wealth in general when processing a withdrawal request and agree to provide all information required by the Company. The Company reserves the right to refuse to process a withdrawal request where a Customer does not provide all required information, and/or where the Company has reasonable concerns that doing so may result in breaches of the anti-money laundering and counter-terrorist financing laws and regulations (AML/CTF Laws).

### ***4 Source of deposit and/or funds***

- 4.1 Customers from **Medium** and **Low Risk** jurisdictions must provide a copy of BOTH SIDES of the credit card they will use to fund the account from.
- 4.2 Customers from **High Risk** jurisdictions must provide proof of all payment methods they will use to fund the account before depositing the funds. Specifically:
- **Credit Card statement copy** if deposit is greater than USD 20,000 (or equivalent currency)
  - **Prepaid cards / cards not displaying a name**, must be accompanied by a statement showing the name of the card owner
  - **Screenshot of e-wallet online portal** for deposits made by e-wallet.

### ***5 Withdrawals***

- 5.1 **Withdrawal to source:** It is the Company's policy that funds are returned to the same source in the same currency to minimise the risk of cross border payments and reducing the risk of being used for money laundering purposes. There may be instances where accounts are opened incorrectly in a different currency to the one required by the Customer. Accounts will be changed to reflect the correct currency. If this is the case, Customers must be aware that they will responsible for any exchange rate differences, unless the error is by the Company.
- 5.2 **All withdrawal requests to debit/credit card:**
- 5.2.1 Debit/Credit Card withdrawal can only be used for the deposit amount made using that Debit/Credit Card.

- 5.2.2 When a deposit is made via Debit/Credit Card and a subsequent withdrawal request is received, the amount of funds sent back to the original Debit/Credit Card, may not exceed the original maximum amount deposited from the same Debit/Credit Card. Any profits made in excess of the deposited amount will be transferred to the nominated bank account; which must be held in the same name as the Customer's trading account. In order for the profits to be sent to the aforementioned bank account a copy of a recent bank statement must be provided.
- 5.2.3 Debit/Credit Card refunds can take between 10 business days from the date of processing to appear on the Customer's statement.
- 5.3 **Withdrawal to third party:** This is not permitted as all funds withdrawn from the Customer's trading account must go to a bank account in the same name as the Customer's trading account.
- 5.4 **Withdrawal to new Bank Account:** A clear copy of a recent bank statement showing the full bank details, with the name and address of the Customer must be provided and where available a copy of an account closure letter from the bank of the old account.
- 5.5 **Withdrawal to new Credit/Debit Card or Payment Wallet:** A clear copy of the front and back of the card (the full long number and the CVV number should be removed) must be provided. The Customer will be asked to provide a letter from the card provider relating to the new/expired card.
- 5.6 **Sufficient funds to withdraw:** Customers can withdraw funds from their trading account when they have a positive cash balance providing that their funds are not being utilised for margin or open losses. The maximum amount of funds that a Customer can be repaid is the cash balance minus the open positions. There are instances where the available funds available will be reduced due to the nature of the positions held, to ensure there are sufficient funds on the account to cover any future margin requirements.
- 5.7 **Currency of withdrawals:** A Customer can make withdrawals from the account in their base currency.
- 5.8 **Withdrawal authorisation:** Once satisfied that the withdrawal is in line with this Policy, additional authorisation may be required depending on the value of the transaction. The following table sets out the approval limits for making withdrawals (levels approved by the Board).
- 5.9 **Withdrawal requests must be in writing:** Customers must request a withdrawal request in writing.

Amount	Level	Required authorisation
Anything under \$5,000 (or equivalent currency)	1	No authorisation required.

Over \$5,000 (or equivalent currency) (inclusive)	2	Account manager conCompanyation.
---	---	----------------------------------

Where there is more than one person required to authorise a withdrawal, each person must complete their own checks and be satisfied withdrawal is okay before passing to the next authority.

Any questions should be referred to the Head of Back-Office – **if in doubt, do not send funds out!**

## 6 Account and Customer Checks

### 6.1 Customer History

Before completing a Customer's withdrawal, the Customer account is reviewed firstly by the back-office payments team, who will carry out a number of initial checks to ensure:

1. That the payment is not a third-party payment
2. That there are no unapproved bonuses on the account
3. The initial deposit was returned to the original source
4. Profits have been sent to an account in the same name as the trading account
5. The next step involves the back-office KYC team carrying out further checks:
  - a. All KYC documents are available and up to date
  - b. Recent World check is conducted
  - c. Where the amount is significant (greater than thirty thousand (20,000) USD or equivalent) the Customer has been contacted to discuss reasons for the withdrawal to ensure that they are no problems or irregularities
  - d. Check that trading has occurred

6.1.1 The withdrawal will then be approved by a member of the back-office team. If there are any issues, the account will be referred to the Head of Back-Office, who will undertake the following tasks:

- a. Check to ensure there is no suspicious or unusual trading or payment activity, which could also be a mistake or an error on the account.
- b. Check for any messages on the account that have previously been written by a member of staff.
- c. Check the incoming and outgoing payment activity and identify any anomalies;
- d. Ensure the deposits were returned to the original source;
- e. Ensure the source of funds are not continually being changed;
- f. Ensure that sufficient trading has occurred on the account prior to withdrawing. Where there has not been any trading, the reason for the withdrawal must be sought from the Customer and the account must be assessed for any other anomalies;

- g. taking further steps to be satisfied that the transaction (payment/withdrawal) is consistent with the purpose and intended nature of the business relationship;
- h. Is the Customer a business that is cash intensive e.g. a casino?
- i. Is the transaction (payment or withdrawal) complex in any way or unusually large e.g. greater than thirty thousand (20,000) USD or equivalent Identify any other red flags the Customer's account is demonstrating;

6.1.2 Once these checks have been completed and any issues have been cleared, the payment can be made to the Customer.

## **6.2 *Suspended/Dormant Accounts***

6.2.1 If the account is suspended, the Company will check the notes on the Customer's account for the reason of suspension or dormant account, before permitting a withdrawal request or accepting any deposits.

6.2.2 The Customer's account may be re-activated if deemed appropriate, for example the reason for the suspension was noted on the Customer's back office account and the reasons is sufficiently acceptable to permit the account to be re-activated.

6.2.3 If an account is dormant and the Customer wishes to withdraw their balance, funds must be sent back to the original source or obtain evidence of the account/card they wish to send funds to.

6.2.4 A fresh PEPs and Sanctions world check must be run on the Customer in such instances and saved on the Customer's Back-Office profile.

## **7 *Fraud Check***

### **7.1 Preventing fraudulent activity:**

The safest method of returning funds is sending them back to their source. If funds cannot be returned to the source, the Company must be satisfied that the reason is genuine (perhaps a bank account has been closed or card details have expired). The Company is cautious to ensure the destination is verified.

The Company is committed to the prevention of fraud and the promotion of an anti-fraud culture. As a result it operates a zero-tolerance attitude to fraud and requires staff to act honestly and with integrity at all times, and to report all reasonable suspicions of fraud. The Company will investigate all instances of actual, attempted and suspected fraud committed by staff, consultants, suppliers, Customers and other third parties and will seek to recover funds and assets lost through fraud. Perpetrators will be subject to disciplinary and/or legal action.

The term 'fraud' is commonly used to describe the use of deception to deprive, disadvantage or cause loss to another person or party. This can include theft, the misuse of funds or other resources or more complicated crimes such as false accounting and the supply of false information by employees, suppliers, consultant, Customers or any other third party.

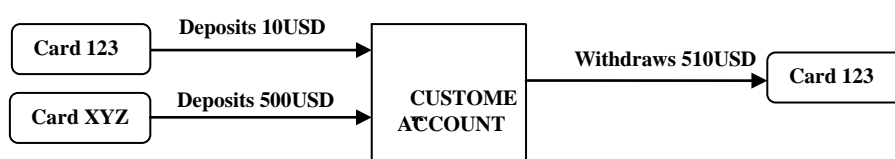


The Company has established procedures to encourage staff to report actual, attempted or suspected fraud and/or other forms of illegal activity without fear of reprisal.

## 7.2 Example of fraudulent activity:

7.2.1 A possible sign of fraud is where a Customer has funded his account with various cards but then requests a refund back to a card which has only been used to deposit a small amount e.g. 10USD, as shown in the example below:

### Example of fraudulent activity

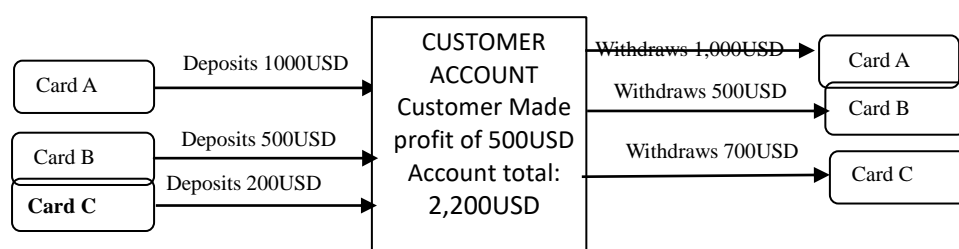


7.2.2 The 500USD deposit should therefore be sent back to the place of origin, i.e. **Card XYZ/Wallet**.

7.2.3 If you see this pattern and cannot return funds to Card XYZ or feel that the funding on an account is unusual, perhaps the account has multiple cards registered to it and has only been open for a few weeks, or if you have any other concerns/suspensions - report these to the Compliance before making a withdrawal.

7.2.4 A likely indication of fraud is where a Customer funds the account with card deposits then places a number of small trades to disguise his payment activity, and then requests the funds back via card, e-wallet or bank wire.

7.2.5 In the example below, if the Customer deposits from a number of different cards, such as Cards A, B and C, the withdrawals should also be conducted in the same proportionate manner. Any profits made on the account will be refunded to the last remaining card on the account.



## 8 Transfer of Funds between Customer accounts

8.1 Customers are able to transfer funds between internal accounts if the following conditions are met:

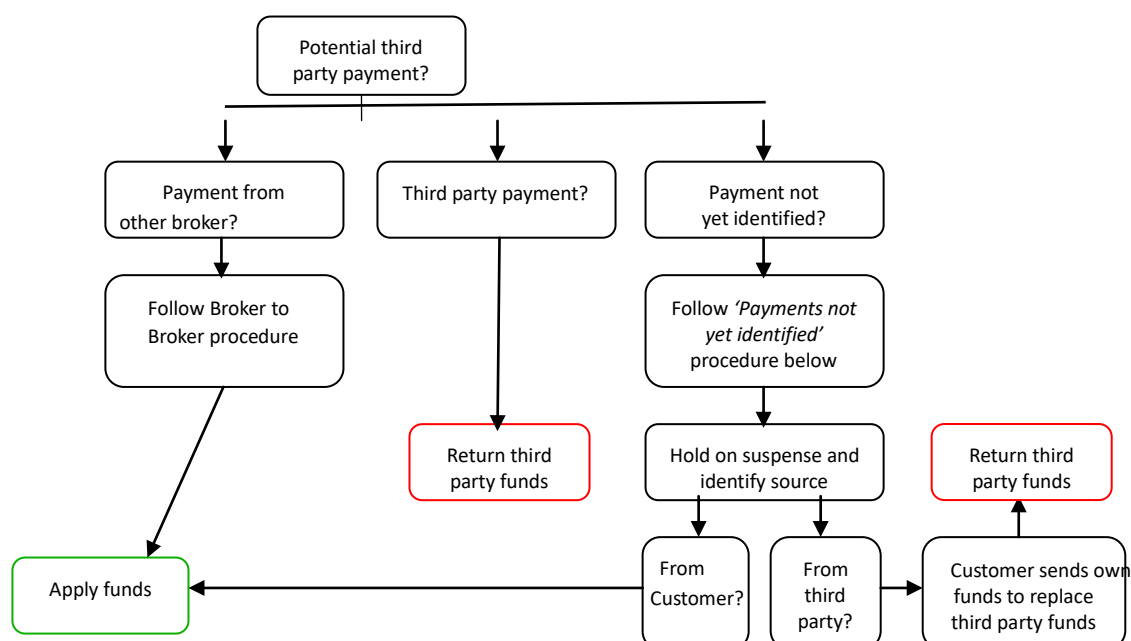
8.1.1 Both accounts are in the same Customer name; AND

8.1.2 The Customer accounts have the same Date of birth; AND

8.1.3 The Customer accounts have the same address.

## 9 Third Party Payments Policy

9.1 The below diagram outlines how various possible 'Third Party Payments' are handled by the Company:



### 9.2 Cash payments

9.2.1 The Company **does not accept cash payments** since they pose a significant money laundering risk to the Company.

### 9.3 Broker to broker payments

9.3.1 Third party payments are prohibited unless to/from Customer's named account at another broker.

9.3.2 A proof of trading account held with the other Company is required, which is usually fulfilled by the Customer's completion of **Blackridge's Broker to Broker transfer form**.

9.3.3 The minimum acceptable requirement is an email confirmation from the other broker, informing us of this move.



## 9.4 Corporate Accounts

- 9.4.1 A corporate account must be funded from an account in the company name.
- 9.4.2 Authorised persons listed on the account are not permitted to fund the account from their personal account, as this would be classified as a third-party payment, which is not permitted.
- 9.4.3 In exceptional circumstances, the beneficial owner or significant controller of the company may deposit from their own personal account, as long as they provide a written confirmation (for example by email) that they are permitted to deposit from their personal account into the corporate account on behalf of the company.

## 10 Payments & Withdrawals Policy

### 10.1 Payments from Family Members

- 10.1.1 There may be instances where family members are nominated by a Customer (spouse, parent or child over 18) to fund the account.
- 10.1.2 The nominated individual will be subject to the usual anti-fraud and AML checks identify verification checks.
- 10.1.3 If the funds are gifted from a family member, there must be a letter from the family member confirming that they are gifting the funds to the Customer.

## 11 Red Flags

**Make sure you know your red flags!**

**Deposits can be suspicious in their own right and must be appropriately managed to prevent the risk of money laundering, fraud and terrorist financing to the Company. However, if a Customer is committing money, money laundering or engaging in acts of terrorist financing, the withdrawal process would be the final stage of the unlawful activity in regard to the Company's role in the process, as such extreme care and due diligence must be applied.**

It can be difficult to detect suspicious transactions, so the Company must remain vigilant at all times. When assessing whether there is a high risk of money laundering and terrorist financing in a particular situation that also looks potentially unusual or suspicious and the extent of the measures which should be taken to manage and mitigate that risk, staff must take account of at least the following risk factors presented below.

If any the answer to any of the questions below is a 'yes', you must investigate further and report it to the Company's MLRO.

Red Flag examples
A Customer uses unusual or suspicious identification documents that cannot be readily verified.
A Customer uses different National Identification Card numbers with/without variations of his or her name.
A Customer refuses or is reluctant to provide appropriate Identification or proof of address documents.
The Customer exhibits unusual concern regarding the Company's compliance with government reporting requirements and the Company's AML policies, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspect identification or business documents.
The information provided by the Customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
Upon request, the Customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
Does the identification document exhibit signs of fraud (tampering with the document)?
The Customer (or a person publicly associated with the Customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
For no apparent reason, the Customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
The Customer has been identified by world check as having a positive result for sanction/adverse media against their name - such as criminal activity.
The prospective Customer (natural person, director, beneficiary or beneficial owner) is named in a government list or a credible source's list (sanctions lists) as identified by World Check?
The Customer one who is a long-standing Customer or only undertakes occasional large transactions or small frequent transactions, which are dated widely apart?
It difficult to identify the true controlling owner of the Customer/entity from the corporate structure or there is no legitimate commercial rationale for the structure.
The Customer insists on or asks for exemptions from the Company's policies relating to the deposits and withdrawals, such as in relation to third party transfers or transfers to an account which is the source from where the funds were originally deposited.
The Customer's account has unexplained or sudden extensive activity, especially in accounts that have had little or no previous activity.
The Customer/IB has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.

There is an unusual pattern of transactions (payments and withdrawals) and the transaction or transactions have no apparent economic or legal purpose?
The Customer requests that a transaction/deposit/withdrawal be processed in such a manner to avoid the Company's normal documentation requirements.
The Customer makes a funds deposit followed by an immediate request that the funds be wired out or transferred to a third party, or to another Company, without any apparent business purpose.
The Customer's account shows numerous transactions/deposits aggregating to significant sums that may or may not be consistent with their financial standing/occupation/savings etc on their application form.
A business/corporate is reluctant, when establishing a new account, to provide complete information about the nature and purpose of its business, anticipated account activity, prior banking relationships, the names of its officers and directors, or information on its business location.
Customer wishes to withdraw their funds into a third-party account in someone else's name.
Customer wishes to withdraw their funds into a new account in their name, but was not the original source of where the funds came from.
The Customer lives in a particular jurisdiction but deposits funds from another jurisdiction which is a higher risk jurisdiction to where the Customer resides.
A Customer deposits funds into several accounts, usually in amounts of less than 3,000 USD, which are subsequently consolidated into a master account and transferred outside of the country, particularly to or through a location on Money Laundering (FATF) as non-cooperative countries and territories or higher risk jurisdictions).
Funds transfer activity occurs to or from a financial secrecy haven, or to or from a higher-risk geographic location without an apparent business reason or when the activity is inconsistent with the Customer's transaction/withdrawal or deposit history.
Customer transfers many small funds and very shortly after withdraws their funds to another bank account in another country in a manner which is inconsistent with the Customer's history.
Large or small funds are deposited into an account or multiple accounts without any trading activity and the funds are soon withdrawn.
The currency transaction patterns show a sudden change inconsistent with normal activities and application information.
Customer makes lots of small deposits and quick withdrawals.
The stated occupation of the Customer is not commensurate with the type or level of activity.

A large number of incoming or outgoing funds transfers take place through a business/corporate account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves higher-risk locations.

Foreign exchange transactions are performed on behalf of a Customer by a third party, followed by funds transfers to locations having no apparent business connection with the Customer or to higher-risk countries.

Funds are received from higher risk jurisdictions on behalf of the Customer or from the Customer's account.

It been determined that a Customer or potential Customer is a Politically Exposed Person, or a family member or known close associate of a PEP.

The structure of the company unusually complex with more than 3 layers of control by beneficial owners?

The Customer has accounts in a country identified as a non-cooperative country or territory by the Financial Action Task Force (FATF) as per the country risk rating matrix.

The Customer's account demonstrated unexplained or sudden extensive bank wire activity (deposits and/or withdrawals), especially in accounts that had little or no previous activity.

The Customer is a company that has nominee shareholders or shares in bearer form.

