

Anti Money Laundering and Terrorist Financing Policy

TABLE OF CONTENTS

1. Introduction	3
2. Purpose	3
3. Scope	3
4. Policy	3
5. Money Laundering	3
6. Money Laundering legal requirements	4
7. Money Laundering offences and obligations	4
8. Bolt's approach	5
9. Third party payments and receivables	6
10. Conclusion	7

1. Introduction

Money laundering is the process by which individuals or entities try to conceal illicit funds, or otherwise make these funds look legitimate. Money laundering is illegal and both domestic and international laws contain numerous anti-money laundering provisions, which apply to Bolt's business.

Terrorist financing ('TF') is the process by which terrorists fund their operations to perform terrorist acts. There are two primary sources of financing for terrorist activities. The first involves financial support from countries, organizations or individuals. The other involves a wide variety of revenue-generating activities, some illicit, including smuggling and credit card fraud.

2. Purpose

This policy provides guidelines on identifying money laundering and terrorist financing; and tools to aid you if you have any concerns about this subject. The policy is designed to mitigate the risk the Company, and all of its partners, face from becoming involved in any business activity where money laundering is taking place.

3. Scope

This Policy applies to all employees, suppliers and customers of Bolt Global Solutions Ltd. Every employee of Bolt is expected to comply with all applicable anti-money laundering regulations. Every Bolt manager is required to take necessary action to ensure compliance with this policy.

Failure to adhere to this policy could result in an employee facing disciplinary action up to and including termination.

4. Policy

Bolt does not facilitate or support any type of activity linked to money laundering. It will only conduct business with third parties, which it believes are not engaged in money laundering or terrorist financing activities and will not knowingly facilitate any transaction that has elements of such practice. Employees must never engage in any type of money laundering activity.

5. Money Laundering

Money laundering is used to conceal the true origin of funds gained through activities such as, but not limited to, fraud, corruption, tax evasion and drug trafficking. If undertaken successfully, the process facilitates the appearance of legitimacy of such funds.

Money laundering can take many different forms, in some cases the transfers involved can be relatively simple whilst in other situations there may be a complex web of transactions.

Generally, there are three main stages: placement, layering and integration.

- 5.1.1. Placements - funds derived from illegal activities are deposited into the financial system. The proceeds of the criminal act need to be introduced into a financial system, for example, paying for high-value goods with cash can arouse suspicion.
- 5.1.2. Layering - Confusing the trail in order to disguise the source and ownership of funds. Once the funds are in the system, criminals complicate the trail to distance themselves from the funds and make it harder to find the funds or the source thereof.
- 5.1.3. Integration - Funds are integrated into the economy appearing legitimate. The funds are now integrated into the economy and are given the appearance of coming from legitimate sources.

6. Money laundering legal requirements

As a global organisation, Bolt applies internationally recognised industry standards to its anti-money laundering procedures, as recommended by organisations such as The Financial Action Task Force ("FATF") and UK's Joint Money Laundering Steering Committee (JMLSG).

Failure to comply with the relevant legal standards can result in criminal sanctions for both individuals and entities including fines and/or imprisonment.

7. Money laundering offences and obligations

summary of the key offences under anti-money laundering regulations, and employee obligations are detailed below.

Assisting a money launderer:

It is an offence to assist a money launderer in any way and as such, the three principal money-laundering offences are included under this umbrella:

- Concealing, disguising, converting or transferring criminal property or removing criminal property from the country of origin.
- Entering into or becoming concerned in an arrangement which the person knows or suspects facilitates the acquisition, retention, use or control of criminal property by or on behalf of another;
- Acquisition, use, and possession of criminal property.

Failure to report:

It is an offence not to report knowledge or suspicion of laundering activity as soon as reasonably possible, when there were 'reasonable grounds' for doing so. Please report any such knowledge or suspicion to admin@bolt.com.zm or the online platform.

Tipping off:

It is an offence to prejudice an enquiry by tipping off the launderer, or anybody else, that a disclosure has been made and an investigation into their activities is being, or may be, carried out.

Summary of our Money laundering obligations:

- Do not 'Tip Off' - Once employees are aware an investigation is underway, they must never disclose this to the counterparty.
- Identify your customer – Completing due diligence/ KYC before entering into a new relationship with a counterparty is compulsory.
- Sanctions Checking – Bolt performs sanction list checking on all new customers before approving the relationship. All existing customers are subject to our ongoing screening procedures as well.

8. Bolt's approach

Two key issues may indicate higher money laundering risk of which all employees should be aware:

- Counterparties' integrity concerns
- Payment irregularities

Counterparty Integrity

Bolt's KYC procedures form the foundation of its anti-money laundering controls and are designed to identify any potential counterparty integrity issues at the very start of any new relationship. Risk-based due diligence in accordance with Bolt's KYC process must be conducted on all potential counterparties to establish their beneficial owners and their sources of income.

The level of due diligence undertaken on a counterparty depends on several risk factors based upon JMLSG guidance. These risk factors include: type/ structure of company; country of incorporation; location of bank account; political connections/exposure; volumes of transactions; and nature of business activity.

For detailed guidance on the risk matrix applied to counterparties and the resulting levels of due diligence required please contact the Compliance Department.

No payment can be made to or received from a third party before the appropriate level of KYC/ due diligence has been completed through the KYC portal found at www.bolt.cm.zm and KYC approval has been confirmed.

The Company's KYC procedures include ongoing monitoring and periodic due diligence reviews for counterparties after they have been initially approved. This is to ensure new risks that develop during the life cycle of a relationship are appropriately considered.

Employees should report concerns that they may have or become aware of to the Compliance department at admin@bolt.com.zm or the online platform.

9. Third party payments and receivables

There are various legal and compliance reasons that Bolt should only accept payment or make payments for goods and/or services from the specific entity with which we have contracted and not any other entity. This is the case even where such an alternative entity is affiliated in some way to the contractual entity. As such:

- Bolt will not receive payments from or make payments to third parties, which are not the parties to the particular business transaction.
- Bolt must make payments to a third party only to the account contractually agreed between Bolt and the third party.
- Except in instances where we are serving the end customer in downstream business, Bolt must not receive payments in cash from third parties for business transactions.
- Bolt will only receive or make payments from or to jurisdictions connected with the particular business transaction or as otherwise agreed in the contract between Bolt and the third party. The Regional Head of Compliance must approve any exceptions to this rule before signing the contract with the third party.
- Bolt will not accept over-payments by a third party and the Finance Manager must approve any request for refunds of money to a third party, which might have overpaid Bolt.
- Any request from a third party for payments to be made to Bolt through multiple forms must be approved by the Finance Department after careful review of the documented justification for such request.
- Any change to previously agreed modes of payment or currency by Bolt must be approved by the Finance Department.

9.1. Exception process

Exceptions to the general rules above should be rare.

The Finance team will not process any third-party payment/request until the relevant employee can demonstrate to the Finance team that they have satisfied the following mandatory conditions:

1. A written explanation must be provided by the counterparty, setting out the reason for the need for a third-party payment/receivable or any deviation to the above rules. Employees are reminded that Bolt will not facilitate tax evasion or breaches of currency controls.
2. Any such third-party entity must complete risk-based due diligence (whether Bolt is making or receiving payment).
3. The Credit team must confirm that payment can be accepted from the third party in question (only where Bolt is receiving payment from a third party, including via LC agent).
4. The relevant contractual arrangements that Bolt has with our actual counterparty must be amended to formally appoint the relevant third party to make/ receive payment, but that recourse for any amount that is unpaid under the agreement continues to rest with the counterparty (such documentation must be signed by Bolt, the counterparty and the relevant third party). Employee must contact the Bolt legal team for completing the contract.
5. Where our counterparty is located in a jurisdiction subject to currency controls, the payments will only be accepted from, or paid to, third-party entities that are located, and using a bank account located, in the same jurisdiction as our counterparty.
6. Where Bolt is being asked to make payment to a third party, the Finance Manager must review and conduct required diligence to verify such third party and their credibility.

The conditions at points 1, 2 and 6 must always be completed. Where any other condition is not satisfied, the Finance (treasury) team should escalate the issue to the (Finance) Treasury Management for guidance. All third-party exceptions will be managed by the Finance Department.

10. Conclusions

If you are ever unsure as to what conduct is acceptable, please contact your manager or one of the Compliance personnel. Alternatively, you can raise the concern through the Bolt email.