Footstock.com - Anti Money Laundering Policy

1. Introduction

1.1 Money Laundering

Money Laundering (ML) is the process of creating the appearance of funds obtained from criminal activity, such as drug trafficking or terrorist activity, being originated from a legitimate source. Criminals attempt to launder money by disguising the source and/or changing the form of the funds, or moving them to a place where they are less likely to attract attention.

1.2 Anti-Money Laundering

Anti-money laundering (AML) is a financial/legal term used to describe the legal controls that require financial institutions and other regulated entities to prevent, detect, and report ML activities.

An effective AML program requires a jurisdiction:

- To have criminalized Money Laundering
- To have given the relevant regulators and police the powers and tools to investigate it
- To have its financial institutions identify their customers, establish risk-based controls, keep records and report suspicious activities
- To be able to share information with other jurisdictions as appropriate

2. Regulation

Employees working in the remote gaming industry are required to make a report in respect of information that comes to them in the course of their business:

- When they know
- When they suspect
- When they have reasonable grounds for knowing or suspecting that a person is engaged in money laundering or terrorist financing, including criminal spend.

Footstock must be able to demonstrate that the extent of the ongoing monitoring undertaken is conducted on a risk-sensitive basis and that all the records are retained by us to reflect this, with risk profiles being properly maintained. In this document, we have identified additional measures that are being applied in order to carry out risk monitoring and the need of where we would require a Declaration of the source of funds from customers in situations which present a high risk and potentially money laundering.

3. Crime & Disorder and AML policy

Our AML policy is based on these principles and practises:

- We develop systems and controls that are appropriate for our business and comply with legal and regulatory requirements

- We assess the AML risks inherent in our current business at least annually; we then adopt a risk-based approach that is flexible, effective, proportionate and cost effective
- We have full commitment for this from, and responsibility resting with, senior management
- We regularly assess the adequacy of our systems and controls
- We maintain records of transactions that meet the needs of law enforcement investigations tackling money laundering and terrorist financing
- We provide initial and ongoing training for all relevant employees
- We support the nominated officer with resources and authority to operate objectively and independently

4. **Risk Management**

We have policy and procedures in relation to risk assessment and management, as required under the Money Laundering Regulations 2007 (the Regulations). This risk-based approach involves a number of discrete steps in assessing the most proportionate way to manage and mitigate the money laundering and terrorist financing risks we face:

- Identify the money laundering and terrorist financing risks that are relevant to us
- Design and implement policies and procedures to manage and mitigate these assessed risks
- Monitor and improve the effective operation of these controls
- Record what has been done, and why

This risk-based approach focuses the effort where it is most needed and will have most impact. It has the full commitment and support of our senior management, and the active co-operation of all employees. We have conducted an assessment of our business risk exposure to money laundering, which considers the threat, and its impact.

5. Suspicious Activity

Suspicious Activity in this case is being referred to as suspicious transactions, extreme player profiles, when deposits are not matching up amongst other elements. Other concrete examples of how we identify players who require our team to undertake a risk monitoring approach of our customers and when to specifically carry out enhanced due diligence checks on the Player Profiles can be further required:

1. Passport or ID card.
2. Utility bill.
3. Bank statement.
4. Other proof of identity.

The Enhanced Due Diligence Checks are subject to players' profile and the amount of Risk they pose to us. Only when we determine some of the above points or a combination of a few will we flag the customer/customers in question and conduct risk monitoring.

5.1 Suspicious Activity Reports SARs

Within that framework, Suspicious Activity Reports (SARs) are an imposed requirement. Footstock ensures that any employee reports to the Compliance Officer where they have grounds for knowledge or suspicion that a person or customer is engaged in ML or terrorist financing. Any employee failing to so do is open to criminal prosecution.

Escalations of SARs should be done in a confidential, discreet manner. An employee must not, under any circumstances, disclose or discuss any AML concern with the person or persons subject to an investigation, or any other person for that matter. Disclosure (also known as "tipping off") is strictly prohibited and carries with it very serious legal penalties.

Furthermore, and in order to keep ourselves protected as much as possible, no remark should ever be left on an account that would give any indication that ML is suspected, a player being entitled, at any point in time, to request the full notes/ remarks on their account.

5.2 Working Procedure

Footstock reviews players spend and game play to check for suspicious activity. Before any withdrawal is processed the following procedures are carried out:

1. The customers deposit history is reviewed to confirm that no suspicious payments have been made to the customer's account. The frequency of deposits and the sum of deposits are reviewed to ensure they are within normal range for the customer based on his depositing history and the general depositing range throughout our network.

2. The customer's turnover is reviewed to observe their spending habits and deposits vs withdrawal amounts and methods.

3. When possible, funds should always be refunded back to the original payment method used by the player to make a deposit.

5.3 Withdrawal Procedure

When reviewing a customer's account prior to withdrawal the agent must answer the following questions in the AML segment in the Risk Entry:

1. Did the player wager?

2. Does the payment Method belong to the player and has the player used it to deposit?

3. Are the customer's transactions and bets in line with expectations for the player?

5.4 Escalation Process

Following the AML policies in place and escalating any suspicious activity, as previously described, are crucial to the company as they protect it from financial losses and ensure that it remains compliant within the different jurisdictions which govern it.

Any activity which appears suspicious, even only slightly, has to be escalated. Not escalating a suspicion of money laundering can lead to criminal prosecution. Further information on our internal procedures can be requested to management.

6. Employees

6.1 Senior Management

Senior management is fully committed to and responsible for the implementation of this policy. Senior management is made aware of their individual personal liability for consenting to, or conniving in, the commission of offences under the Regulations, or where such offence is attributable to any neglect on his part.

6.2 MLRO

A designated Money Laundering Reporting Officer takes responsibility for SARs in respect of the prevention and detection of money laundering, counter terrorism financing and our obligations under the Proceeds of Crime Act 2000. The nominated MLRO has responsibility for making reports to senior management on anti-money laundering (AML) and countering terrorist financing (CTF) activity, receiving disclosures from employees under Part 7 of the Proceeds of Crime Act 2002 (POCA) and Part III of the Terrorism Act 2000 (the Terrorism Act); and if appropriate, making such external reports.

The MLRO has the authority to act independently in carrying out their responsibilities and has access to sufficient resources to carry out their duties.

Money Laundering Reporting Officer:
Name: Tilmann Weischer
E-mail: tilll@footstock.com
Phone: 00491713577455

6.3 Staff training

All staff will receive training on their obligations in respect of money laundering reporting and are aware of the procedures in place for escalation of any suspected incidents to the MLRO. As part of this process, staff are made aware that personal disregard for the legal requirements, for example, turning a blind eye to a customer spending criminal proceeds, may result in criminal or regulatory action.

7. High Risk Jurisdictions

High risk countries are those countries identified as such by publications issued from time to time by the Financial Action Task Force; or additionally those so identified by the Gambling Commission. Client registered in High Risk Countries are always subject to EDD.

Countries currently on the FATF list are:

- Afghanistan
- Algeria
- Angola
- Bosnia & Herzegovina
- Ecuador
- Guyana
- Iraq
- Iran
- Lao PDR
- Myanmar
- Panama
- Papua New Guinea
- Syria
- Uganda
- Yemen
- DPR of North Korea

Players from the FATF list of jurisdictions seen to threaten the international financial system from on-going and substantial money-laundering or terrorist financing activities, as identified on FATF publications, will be refused.

8. Record keeping

We ensure that there is an audit trail to assist in any financial investigation by a law enforcement body. Our record keeping policy and procedure covers records areas such as KYC and information verification, Internal and external SARs, contacts between the Compliance offer and licensing/enforcement entities, among others.

9. Offences

All employees are made aware of their risk of committing the following related offences:

- POCA and the Terrorism Act create offences of failing to report suspicious activity
- Where an employee fails to comply with the obligations to make disclosures to a nominated officer
- They may also commit an offence under POCA or the Terrorism Act if they disclose information that an SAR has been submitted that is likely to prejudice any investigation
- They also commit an offence if they know or suspect that an appropriate officer is acting (or proposing to act) in connection with a relevant investigation which is being or is about to be conducted, and they falsify, conceal, destroy or dispose of documents which are relevant to the investigation

10. Vetting procedures for new employees

The company undertakes a number of vetting procedures when staff are employed. We will ensure the employee is not a minor through proper identification checks and we will verify the identification and credentials of the employee through at least two independent references. We will also look to verify any further personal information or background information.

11. Protecting our equipment from internal crime and criminal misuse

The company is very aware that a key way to combat fraud is to first identify where the company's most valuable assets are. Processes and controls have been built into the routine business of the company to minimize the chances of any of the key assets being misused.

Our server equipment suppliers have in place necessary policies around protection of equipment, for example, a visitors management procedure, fire alarms, shredding of confidential documents, locked cabinets, testing, a security team etc.

12. Compliance and Risk Committee

We intend to establish this to review executive risk. Both the MLRO and Compliance Officer will be members as will another non-executive director. These will meet no less than quarterly or as required.

13. Ensuring the companies we deal with are trustworthy and reputable

Footstock promotes strong principles of business and professional ethics at every level. When selecting suppliers, there are a number of criteria we consider:

- Financial strength (for long term sustainability);
- Legal and regulatory compliance;
- Commitment to a wider corporate responsibility program;
- Desire and ability to deliver quality and value.

14. Our responsibilities under the Proceeds of Crime Act (POCA)

Footstock is fully aware of the procedures and policies required by the Proceeds of Crime Act 2002 and have policies and procedures in place related to this Act (as detailed below).

15. Internal record keeping

The below key principles: know your customer, internal record keeping and reporting, ensure our compliance with laws and regulations.

- Records on all customer transactions - regardless of their relation to payments or plays - will be kept for at least 6 years after the transaction.
- Records on customer details - regardless of their value state or open/blocked status - will be kept for at least 6 years after the relationship was terminated.
- Records on money laundering investigations and suspicious activity reports will be kept for 6 years after the investigation was completed.

16. Prevention of collusion and data protection compliance

Footstock Terms and Conditions make clear that cheating will not be tolerated and that customer accounts will be closed if cheating occurs. Footstock employees have no access to user payment information. All Customer Information in the organization will be protected through a strict Information Security policy that all employees and suppliers will adhere to, that will include System Access and Authentication Control, Password Policy, Malware Protection measures, Intrusion Prevention policy, Encryption Policy, and strict Network Control and Management.