

Nova Technology BV

**Anti-Money Laundering and Prevention of
Crime Policy**

Contents

- 1. Introduction**
- 2. Legislation & UKGC Guidance**
- 3. Recruitment & Training**
- 4. Reporting**
- 5. Record Keeping**
- 6. Protecting the Company from being a Victim of Crime**
- 7. Appendix 1 (Suspicious Transaction Report Templates)**

1. INTRODUCTION

Policy objectives

- 1.1 Nova Technology BV (the “Company”) is committed to achieving a high standard of regulatory compliance in relation to preventing its services from being associated with crime and disorder. The purpose of this document is to minimise the risk of the Company being used to launder money, assisting in the financing of terrorism or being a victim of crime. This document sets out the Company’s policies in this area, so that management and staff are aware of their obligations and the procedures that must be followed.
- 1.2 As a B2C operator, the Company will have a direct relationship with its players. The Company will satisfy itself and the Curacao Commission (‘CGCB’) that its B2C operational team they are complying with the AML requirements regarding persons that play its games, via its B2C websites.

What is money laundering?

- 1.3 The Company appreciates that the term ‘money laundering’ covers wide-ranging circumstances involving any activity concerning the proceeds of any crime; these include trying to turn money raised through criminal activity into ‘clean’ money, possessing or transferring the benefit of acquisitive crimes such as theft and fraud, possessing or transferring stolen goods, being directly involved with any criminal or terrorist property, or entering into arrangements to facilitate the laundering of criminal or terrorist property, and criminals investing the proceeds of their crimes. It also includes spending the proceeds of crime, as opposed to merely concealing or converting it.
- 1.4 As currently we are following UK legislation, money laundering is defined¹ as an act which:
- a) constitutes an offence under section 327, 328 or 329 of the Proceeds of Crime Act 2002 (“POCA 2002”);
 - b) constitutes an attempt, conspiracy or incitement to commit an offence specified in paragraph (a);
 - c) constitutes aiding, abetting, counselling or procuring the commission of an offence specified in paragraph (a); or
 - d) would constitute an offence specified in paragraph (a), (b) or (c) if done in the UK.
- 1.5 For something to constitute a predicate offence it needs to be an offence in the United Kingdom. Spending proceeds of crimes committed abroad will not constitute money laundering if the relevant crime is not an offence in the United Kingdom.

What is terrorist financing?

- 1.6 Terrorist financing is defined in the Fifth EU AML Directive as the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any terrorism offences. Terrorist financing can involve funds with a legitimate origin.

What other crime might affect us?

- 1.7 This policy also sets out procedures to minimise the risk of the Company being a victim of crime. Crimes that might be perpetrated against the Company include:
- a) unlawful entry to Company premises and/or unauthorised use of Company equipment;
 - b) criminal damage to or theft of the Company's property;
 - c) violence against members of staff; and
 - d) cyber-crimes including hacking, data theft and theft of customer funds.

Nominated officer for AML and associated purposes

- 1.8 The nominated officer for AML and associated purposes (the "Nominated Officer"), at the Company is a designated MLRO. Any changes to this information will be reported to the CGBC as a key event pursuant to licence condition [15.1]
- 1.9 The Nominated Officer's duties and obligations include:
- a) identifying money laundering and terrorist financing risks relevant to the Company;
 - b) designing and implementing policies and procedures to manage and mitigate these risks and keeping these policies and procedures up to date and under review;
 - c) monitoring the effectiveness of the Company's policies and procedures, with consideration to efficiency, employee adherence and system compliance and suitability;
 - d) liaising with and reporting on the effectiveness of the Company's controls, policies and procedures to senior management on a regular basis;
 - e) record keeping;
 - f) training employees in accordance with the staff training policy so that they are aware of the Company's policies and procedures in this area and the reporting structure;
 - g) ensuring compliance with the relevant legislation, regulations and Gambling Commission guidance; and
 - h) reviewing and investigating suspicious transaction reports ("STRs") from staff members, considering whether suspicious activity reports ("SARs") should be submitted to the National Crime Agency ("NCA") and, where appropriate, submitting SARs and requesting appropriate consent to proceed with transactions.

Senior management

- 1.10 The Company's senior management is fully committed at all times to ensuring the effectiveness of policies and procedures relating to anti-money laundering ("AML") and counter-terrorist financing ("CTF"), which will reflect and promote a risk-based approach.
- 1.11 Senior management will fully support the Nominated Officer and will encourage active co-operation from all employees. Senior management will ensure that the Company's policies and procedures are clearly communicated to employees. Further, they will ensure robust mechanisms are in place to ensure the policies and procedures are carried out effectively, all weaknesses are identified, improvements are made where necessary.
- 1.12 Any senior management decisions will be documented to ensure there is evidence of the decision-making processes and an audit trail.
- 1.13 The CFO acting as the Nominated Officer has been appointed as the officer responsible for the Company's compliance with the MLRs. Any changes to this information will be reported to the Gambling Commission.

2 LEGISLATION AND U.K GAMBLING COMMISSION GUIDANCE

The "Relevant Legislation"

UKGC (LCCP) Legislation

- 2.1 One of the three licensing objectives of the OGRA Legislation is preventing gambling from being a source of crime or disorder, being associated with crime or disorder or being used to support crime.

Fifth EU Money Laundering Directive and Money Laundering Regulations 2020

- 2.2 The Fifth EU Money Laundering Directive ("5MLD") has been implemented into United Kingdom law in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2020 (the "MLRs"). Casinos are a "relevant person" under the MLRs.

Proceeds of Crime Act 2002

- 2.3 POCA 2002 sets out offences and penalties in relation to money laundering.

Terrorism Act 2000

- 2.4 The Terrorism Act 2000 sets out counter-terrorism legislation, offences and penalties.

Offences, penalties and defences

- 2.5 Part 7 of POCA 2002 came into force in February 2003 and sets out offences in relation to money laundering which include:

Offence	Legislative Provision	Maximum Penalty	Defence
Concealing, disguising, converting, transferring or removing (from the United Kingdom) criminal property (i.e. cash, goods, real estate)	s. 327 POCA	14 years and/or unlimited fine	Making an authorised disclosure to the nominated officer
Making arrangements which facilitate the acquisition, retention, use or control of criminal property by or on behalf of another	s. 328 POCA	14 years and/or unlimited fine	Making an authorised disclosure to the nominated officer
Acquisition, use or possession of criminal property	s. 329 POCA	14 years and/or unlimited fine	Making an authorised disclosure to the nominated officer
Entering into or becoming concerned in arrangements which facilitate the retention or control by or on behalf of another person of terrorist property	s.18 Terrorism Act	14 years and/or unlimited fine	Proving that you did not know and had no reasonable cause to suspect that the arrangement related to terrorist property
Failure to disclose, knowing or suspecting or having reasonable grounds for knowing or suspecting that another person is engaged in money laundering or terrorist funding	s. 330 POCA & s.21A Terrorism Act	5 years and/or unlimited fine	Reasonable excuse for not disclosing
For an MLRO, failing without reasonable excuse to report a suspicion of money laundering to the NCA	s. 331 POCA	5 years and/or unlimited fine	
Tipping-off any person that a disclosure has been made, knowing or suspecting that doing so is likely to prejudice an enquiry	s. 333A POCA	5 years and/or unlimited fine	
Failure to comply with any relevant requirement of the MLRs (for example not conducting necessary CDD on customers)	r. 86 MLRs	2 years and/or unlimited fine	Taking all reasonable steps and exercising all due diligence to avoid committing the offence
Making a disclosure which is likely to prejudice an investigation or destroying/concealing/falsifying relevant documents	r. 87 MLRs	2 years and/or unlimited fine	Not knowing or suspecting that the disclosure was likely to prejudice the investigation or making it in compliance with a requirement, not knowing or

			suspecting documents are relevant
Providing information which is false or misleading in purported compliance with a requirement of the MLRs or disclosing information in contravention of a requirement	r. 88 MLRs	2 years and/or unlimited fine	Reasonably believing that the disclosure was lawful or that the information had already and lawfully been made available to the public

Gambling Commission Guidance

- 2.6 The UK Gambling Commission has published the fifth edition (January 2020) of 'The Prevention of Money Laundering & Combating the Finance of Terrorism'
- 2.7 It is an ordinary code provision to comply with UKGC Guidance. Whilst this is not legally binding, failure to follow Gambling Commission Guidance would be taken into account as part of any investigation into AML failings or licence review. The Company's policy is therefore to adhere to Gambling Commission Guidance and its provisions have been incorporated into this document.

Gambling Commission public statements

- 2.8 In recent years there have been a number of high-profile public statements relating to AML and social responsibility controls. The latest list of relevant public statements is set out below:
- **Hillside (UK Gaming) (2024)**
 - **Lindar Media Ltd (2023)**
 - **Done Brothers (Cash Betting Ltd) (2023)**
 - **Video Slots Ltd (2023)**
 - **Skill on Net (2023)**
 - **William Hill Org Ltd (2023)**
 - **Mr Green Ltd (2023)**
 - **Blue Star Planet Ltd (2023)**
 - **Vivaro Ltd (2023)**
 - **Spreadex Ltd (2022)**
 - **Ladbrokes Betting & Gaming Ltd (2022)**
- 2.9 We understand that the issues identified in the public statements provide valuable learning for us and provide indicators of bad/good practice. As these public statements mainly concern B2C operators,

3 APPROACH TO AML AND COUNTERING TERRORIST FINANCING

Risk-based approach

- 3.1 The Company has adopted a risk-based approach to AML and counter terrorist financing (“CTF”), with the aim of managing and mitigating money laundering risks in a proportionate way. We understand that the Regulations and Gambling Supervision Commission Guidance require us to have policies and procedures in relation to risk assessment and management.
- 3.2 The 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. These steps include:
- a) identifying the risks that are relevant to the business;
 - b) designing and implementing policies and procedures to manage and mitigate these assessed risks;
 - c) monitoring and improving the effective operation of these controls; and
 - d) recording what has been done, and why.
- 3.3 A money laundering and terrorist financing risk assessment will be carried out and documented, which considers the risk level of our products, services, customers and the geographic location of the Company’s activities. The aim of this risk assessment is to identify and quantify risks and to determine how these risks should be managed and mitigated.
- 3.4 We appreciate that the risk-based approach requires the full commitment and support of senior management. Most importantly, we understand that in addition to the existence of policies and procedures, we need to ensure we have robust mechanisms in place to ensure that they are carried out effectively. Where weaknesses are identified, we make the necessary improvements.
- 3.5 UKGC Licence condition 12 requires us to:
- a) conduct an assessment of AML risks to our business as our business changes;
 - b) use the assessment as a tool to develop our policies, procedures and controls; and
 - c) ensure our policies, procedures and controls are implemented effectively and revised to ensure they remain effective following our learning or guidelines from the Commission.

Dynamic assessment of risk

- 3.6 The Company appreciates that its money laundering and terrorist financing risk assessment is not a one-off exercise and that its policies and procedures must be kept under regular review.
- 3.7 The nature of risks and threats changes over time; it is therefore important that we adopt a continuous process to consider these, learn and adapt. Given that the risks posed to our business will continually change, it is important that we review our data management strategies and use of technology to ensure we are adopting the best systems.
- 3.8 We intend to review and revise this document **at least annually**, and also when there is any change to the Relevant Legislation and/or further guidance releases from the UK Gambling Commission.

4 RECRUITMENT AND TRAINING

- 4.1 Any employee who is able to affect the Company's compliance with the Relevant Legislation or is otherwise capable of contributing to the identification or mitigation of the risks of money laundering and terrorist financing or the prevention or detection of money laundering and terrorist financing (a "Relevant Employee") will be subject to an assessment of their relevant skills, knowledge, expertise, conduct and integrity, both before appointment and during the course of their employment.
- 4.2 Relevant Employees will receive regular training to ensure they are:
 - a) made aware of the law relating to money laundering and terrorist financing, and to the relevant requirements of data protection; and
 - b) able to recognise and deal with transactions and other activities or situations which may be related to money laundering or terrorist financing.
- 4.3 A written record of the training undertaken will be maintained.

5 REPORTING

Suspicious activities

- 5.1 UK Gambling Commission Guidance and Relevant Legislation confirms when a report should be submitted, namely where the Company:
 - a) has knowledge of money laundering. This is an objective test, which means that we actually know something is true. Knowledge can be inferred from surrounding circumstances, but it must have come to us in the course of business;
 - b) suspects a person has engaged in money laundering. Again, this is an objective test. There is no requirement for the suspicion to be clear or firmly grounded on specific facts, but there must be a degree of satisfaction. Therefore, if the Company suspects a customer, is laundering the proceeds of crime, it must report regardless of the basis for the suspicion; or
 - c) has "reasonable grounds to suspect or know". This is a subjective test, which means that we have to ask whether "a reasonable person working in a Gambling Operation had specific knowledge or specific suspicion, or had knowledge or suspicion of criminal activity..."
- 5.2 The Company acknowledges and understands that a variety of factors can lead someone either to know or suspect that they are dealing with the proceeds of crime. For instance, as outlined in the LCCP Guidance, this may range from knowledge of a customer's spending habits to an awareness of the source of their funds.

Internal reporting - suspicious transaction report

- 5.3 Any employee who suspects money laundering activity **must** report their suspicions promptly to the Nominated Officer (Money Laundering Reporting Officer, “MLRO”) using a STR. This is an internal report only.
- 5.4 A standard template STR is available in Appendix 1. It must include full details of the customer who is the subject of concern, details of gambling transactions, details of source of funds (if available) and details giving rise to the grounds for knowledge, suspicion or reasonable grounds to know or suspect.
- 5.5 All STR’s and associated correspondence will be documented and electronically recorded at all times.
- 5.6 It is important that the party subject to our suspicion is not notified of any suspicion or investigation, as any discussion of this nature would put the Company at risk of committing the offence of tipping off. Care must be taken in discussing a suspicion and discussions should generally only be held with the MLRO.
- 5.7 In considering whether there are grounds for knowledge or suspicion, the Guidance provides that the MLRO may also require further information to be obtained and if necessary, do so from the customer.
- 5.8 It is the Nominated Officer’s responsibility to decide whether or not to make an external report to the NCA.

External reporting - suspicious activity report

- 5.9 Once an STR has been received, the MLRO will review it and consider whether or not, in his/her view, the activity is at risk of money laundering. If necessary, the Nominated Officer will discuss with the internal reporter or customer service any further information that should be obtained from the customer. Any requests will be handled sensitively and discretely.
- 5.10 The Company must consider whether it should temporarily suspend or permanently cease transacting with a party whom it suspects of money laundering. The Company will not be tipping off the party by terminating a transaction; it is free to terminate its business relationship with a party if it wishes, subject to any termination provisions in a contract, and provided this is handled sensitively there will be no risk of tipping off. To avoid the offence of tipping off, the Company **must not** indicate to the other party that it is considering a report to the NCA.
- 5.11 The MLRO will document his/her reasoning in full.
- 5.12 If the MLRO decides to submit a SAR to the NCA, they will complete the necessary external reporting form following the NCA Guidance. As a basic guide, the SAR will include full details regarding the activities (including relevant dates, deposit and withdrawal amounts) that led the Company to be suspicious and how/why the Company became suspicious. The NCA’s advice is to provide as much detail as possible even if it seems irrelevant, as it could be a valuable piece of information.

- 5.13 Once a SAR has been submitted, it will be reported to the Gambling Commission within five working days via e-Services.

Appropriate consent

- 5.14 If the Company handles any proceeds of crime, they may commit one of the principal money laundering offences as set out in POCA 2002 or the Terrorism Act. However, if the MLRO makes an external report to the NCA this can amount to a defence. This defence includes the statutory mechanism which allows the NCA either to agree to the transaction going ahead, or to prevent the suspect money laundering going ahead. This is called “appropriate consent”.

Avoiding “tipping off”

- 5.15 As set out above, it is essential that all staff understand the importance of not informing or warning third parties that their transactions have been noted and/or reported, either internally or externally. Tipping-off is a criminal offence pursuant to POCA 2002 and subject to a maximum penalty of 5 years and/or an unlimited fine.

Annual report

- 5.16 To ensure robust mechanisms are in place to confirm AML policies and procedures are carried out effectively, the weaknesses are identified, reviewed and improvements are made where necessary. The MLRO will compile an annual report to assist senior management with this task and it will cover the operation and effectiveness of the Company’s AML policies and procedures. The annual report will also include information relating to the number of internal/external reports submitted, any training requirements and any perceived weaknesses.

6 RECORD KEEPING

Importance of record keeping

- 6.1 It is essential that proper records are kept on due diligence carried out on B2C/B2B operator partners, evidence gathered, the decisions that are reached and the reasons for those decisions.

Supporting documents to be retained

- 6.2 The following records will be kept:
- a) Due diligence information;
 - b) Information relating to suspicious transactions;
 - c) MLRO reports;
 - d) Training on AML matters; and
 - e) Policies and procedures.
- 6.3 The source of any information obtained will be recorded along with the information.

Retention period

- 6.4 Records will be retained for at least 5 years from the date of the relevant transaction.

Format

- 6.5 Records will be kept in electronic form as PDF copies of scanned documents or PDF copies of written reports format.

7 PROTECTING THE COMPANY FROM BEING A VICTIM OF CRIME

Physical security measures

- 7.1 The Company will install for example the following security measures to ensure the physical safety of its employees and protect its premises and equipment from unlawful access, damage or misuse: a remote monitored alarm system, CCTV cameras and storage safes. (The specific security measures are yet to be determined.)

Electronic security measures

- 7.2 The Company has yet determined what electronic security measures will be implemented to protect it from cyber-crimes including hacking, data theft and theft of customer funds. However, a few examples are given below demonstrating what measures can/should be taken to prevent cyber-crimes:
- a) Security awareness: All developers are made aware of the impact their actions have on security and privacy. The production infrastructure is set up to disallow unnecessary access;
 - b) Information security: All passwords are generated and strong. Developers and other stakeholders will only be given access to parts of the system deemed absolutely necessary;
 - c) High Availability: AWS handles a lot of the complexity involved with hosting an online web system, such as responding to denial-of-service attacks, floods, fires, hurricanes or any other potential disruption of service and the application itself is set up for high availability;
 - d) Change management: All parts of the system are version controlled, including the infrastructure for hosting the deployed system (infrastructure as code); and
 - e) Remote access: This is made through a bastion server, only accessible from certain IP addresses. Neither the back office nor the admin parts of the system are directly exposed to the internet.

APPENDIX 1 - TEMPLATE SUSPICIOUS TRANSACTION REPORT

FOR INTERNAL COMPLETION ONLY

CONFIDENTIAL

Employee details:

From	
Position	
Contact details	
Date of report	

Third Party details:

Full name	
Company	

Nature, value and timing of activity involved:

[Please include full details e.g. what, when, where, how etc.]

Nature of suspicions regarding such activity:

[Please include full details]

Has any investigation been undertaken (as far as you are aware)?

☐ Yes ☐ No

If yes, please include details below:

--

Have you discussed your suspicions with anyone else?

☐ Yes ☐ No

If yes, please specify below, explaining why such discussion was necessary:

Other information:

Signed: _____ **Dated:** _____

Please do not discuss the content of this report with anyone you believe to be involved in the suspected money laundering activity described. To do so may constitute a tipping off offence, which carries a maximum penalty of five years' imprisonment.

FOR COMPLETION BY THE NOMINATED OFFICER

Date report received: _____

Date receipt of report acknowledged: _____

Consideration of STR:

Does the Company have knowledge of money laundering?

☐ Yes ☐ No

Does the Company suspect money laundering?

☐ Yes ☐ No

Are there reasonable grounds for suspecting or knowing money laundering activity?

☐ Yes ☐ No

If yes, please provide full details:

If yes, please confirm date of report to the NCA: _____ and complete the box below:

Details of liaison with the NCA regarding the report:

Is consent required from the NCA to any ongoing or imminent transactions which would otherwise be prohibited acts?

☐ Yes ☐ No

If yes, please confirm full details in the box below:

Date consent received from the NCA: _____

Date consent given by you to employee: _____

If there are reasonable grounds to suspect money laundering, but you do not intend to report the matter to the NCA, please set out below the reason(s) for non-disclosure:

Date consent given by you to employee for any prohibited act transactions to proceed:

Other relevant information:

Signed: _____ **Dated:** _____

THIS REPORT TO BE RETAINED FOR AT LEAST FIVE YEARS