

ELITE TURF CLUB, LLC
ANTI-MONEY LAUNDERING MANUAL

1. Introduction

1.1 Policy

It is the policy of Elite Turf Club, LLC (“ELITE”) to prohibit and actively prevent money laundering, and any activity that facilitates money laundering, or the funding of criminal or terrorist activities, across any ELITE operation, and to comply with (a) all anti-money laundering (“AML”) requirements under the Bank Secrecy Act (“BSA”) and (b) all rules/recommendations promulgated by the U.S. Office of Foreign Assets Control (“OFAC”) and the US Financial Crimes Enforcement Network (“FinCEN”).

This Anti-Money Laundering Manual (this “Manual”) and the ELITE AML program in general enjoy the support of Elite management, all of whom strive to maintain a culture of compliance within Elite.

This Manual applies to:

- Elite Turf Club, LLC, a Nevada limited liability company which conducts certain services for Elite Turf Club, N.V. pursuant to a Management Agreement

1.2 What This Manual Covers

This Manual describes ELITE’s risk-based AML program, and includes the following:

- A description of what money laundering is, and our legal obligations to combat it;
- Specific examples of money laundering;
- Overview of the officers responsible for implementing this program;
- Record keeping requirements applicable to ELITE;
- Customer due diligence procedures (Know Your Customer);
- BSA reporting obligations for account wagering entities;
- Internal controls, policies, and procedures specific to account wagering entities to assure ongoing compliance; and
- Internal and/or external independent testing for compliance.

1.3 Compliance with this Manual is a Condition of Employment

Compliance with this Manual is a strict condition of employment at ELITE. All ELITE employees must also play an active role in preventing the use of ELITE’s services and assets for illicit activity.

Failure to comply with the provisions of this manual may result in disciplinary action, including suspension and/or dismissal.

1.4 MLRO

Audrey Kauffman is ELITE’s Money Laundering Reporting Officer (“MLRO”). Ms. Kauffman can be contacted via email at audrey.kauffman@stronachgroup.com. As MLRO, Ms. Kauffman works with Elite’s management to ensure that all of ELITE’s matters subject to AML regulations are in compliance with applicable laws and regulations. The duties of the MLRO include, among other things, aiding in the monitoring of ELITE’s overall compliance with AML obligations and

overseeing a corporate policy, which policy includes communication concerning AML responsibilities and day-to-day compliance.

Most importantly, the MLRO works with ELITE's management to assess and document the risks related to money laundering using ELITE's platform, while also documenting and implementing mitigation measures to address those risks.

1.5 Independent Testing and Auditing

ELITE recognizes that to maintain an effective AML compliance program it must implement an independent system to (i) verify that management and employees are following the policies and procedures set forth in this Manual, and (ii) detect any deficiencies in said policies and procedures. Consequently, at the discretion of ELITE's management and MLRO, or when necessitated by a significant change to ELITE's platform and/or operating environment, independent testing of the AML compliance program will be conducted by internal audit or qualified external consultants. This independent testing will be risk-based and tailored to ELITE's unique business model while covering all elements of ELITE's AML program, including, but not limited to, customer due diligence, transaction monitoring, required reporting, record keeping, and training. ELITE will cooperate fully with all consultants and compliance reviewers, and with any federal and state regulatory examination staff throughout this process.

On completion of testing, the auditor/consultant will report its written findings to ELITE's management and the MLRO, who will work together to address any resulting recommendations. ELITE's management will also document whether recommendations were followed and, if not, why not and what steps should be taken to address the issue.

2. What is Money Laundering

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally-derived proceeds, such that unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets (in ELITE's case, typically gambling winnings).

Money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is introduced into a traditional or non-traditional financial institution, such as a casino, or into the retail economy. At the "layering" stage, the funds are transferred into a different form, institution, or account, typically through multiple complex financial transactions that conceal the true origin of the funds and eliminate any potential audit trail. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. Terrorist financing may not involve the proceeds of criminal conduct, but can instead involve an attempt to conceal the origin or intended use of the funds, which funds will later be used for criminal purposes.

Although money laundering is often associated with narcotic trafficking, it can also involve other types of criminal activity, including:

- Terrorism
- Bribery
- Extortion
- Organized Crime

- Racketeering (“RICO” (Racketeer Influenced and Corrupt Organizations Act))
- Fraud
- Forgery
- Counterfeiting Currency
- Smuggling
- Piracy
- Tax Evasion
- Transportation of Stolen Property

Importantly, although this policy is labelled an “anti-money laundering” policy, it is meant to broadly address prevention, detection and reporting of all forms of illicit finance that occurs by, at, or through any ELITE component.

3. Risk Assessment

3.1 Overview

ELITE’s AML program is built around management’s/the MLRO’s assessment of individualized AML/CFT risks facing ELITE given the company’s unique combination of services, customers, and geographic locations.

3.2 The Role of Each Employee, Including Supervisors

ELITE’s employees should look for patterns of customer behavior that may suggest the risk of money laundering. Employees should look for a customer’s departure from his or her ordinary pattern of wagering, and should scrutinize suspicious transactions that cannot be readily explained.

Some examples:

- A customer’s betting activity or his financial transaction activity increases significantly without explanation.
- A customer appears to be coordinating his gaming with another customer(s)
- A customer abruptly changes the methods used for depositing/withdrawing funds, or unexpectedly uses multiple sources/destinations for funds.
- A customer funds his/her account in large amounts and has little to no play before withdrawing these amounts.

IF YOU SEE SOMETHING SUSPICIOUS, SAY SOMETHING TO YOUR SUPERVISOR.

3.3 Potential Suspicious Activity

Regulators have identified certain suspicious activities that may occur in gaming and wagering facilities that may invite further internal inquiry and trigger reporting obligations. The following list is not exhaustive, and any determination of what may constitute suspicious activity will vary depending on the specific circumstances, including the amount of the transaction, the identity of the customer, and the nature of the particular transaction.

Red flags that signal possible money laundering or terrorist financing occurring on ELITE's platform include, but are not limited to the following:

- Minimal gaming despite large financial transactions with the entity;
- Structuring of transactions to stay at or slightly below reporting thresholds;
- A transaction that has no apparent business or lawful purpose;
- Presenting a third-party check or wire transfer – whether apparently deriving from a business or an individual – for use in gambling-related activity.
- A negotiable instrument or wire transfer is presented for the benefit of multiple customers, or multiple customers engage in play on a single customer account;
- A customer refuses to provide required information or identifying information;
- A customer requests information about how to avoid regulatory reporting requirements;
- Law enforcement agencies deliver to ELITE a formal request for records, such as a subpoena, or make informal inquiries concerning the customer;
- News articles or other media reports alleged acts of financial wrongdoing by the customer;
- A customer raises his or her financial transactions to levels well above the ordinary levels for that customer;
- A customer requests establishment of an account in the name other than the one by which ELITE knows the customer;
- A customer attempts to deposit front money or to make payments using complex means, such a multiple source of funds or multiple methods of transmission, which could mask the source of the funds transmitted;
- A customer presents funds which ELITE has a basis for suspecting to be the proceeds of illegal activity;
- A customer furnishes a legitimate type of identification document ELITE believes is false or altered (e.g., address changed, photograph substituted) in connection with the completion of a report or another regulatory requirement;
- A customer, who is a big winner, enlists another individual (who is *not* a partner of the customer in the gaming activity) to withdraw a portion of the money won to avoid the filing of regulatory reports or other forms;
- A customer offers a bribe in the form of a tip or gratuity to an ELITE employee, or requests that an employee structure a transaction to evade the filing of a report;
- A customer exhibits unusual interest in ELITE's reporting policies or inquiries about how ELITE's business day is calculated;
- After being told upon attempting to withdraw funds of the necessity to file a report, a customer appears unusually nervous or decides not to withdraw.

3.4 Customer Due Diligence

ELITE's approach to AML is driven by identifying customers and transactions that pose the greatest risk of money laundering so that such customers/transactions can be more carefully scrutinized, when appropriate.

Customers have to provide valid, current, government-issued photo identification (driver's license, passport, alien registration card, state issued ID card) and a permanent address. PO box addresses are not acceptable.

If the customer is a U.S. citizen, or a U.S. resident with a Social Security Number, a Social Security Number is also required. U.S. citizens or residents refusing to provide a social security number, or who are believed to have provided Elite with false identification information, will not be allowed to wager with Elite and will trigger Elite's filing of a Suspicious Activity Report ("SAR"). At this point, the filing of a report to the Financial Intelligence Unit ("FIU") will be made as well.

For high-volume customers or transactions identified as having potential AML risk, ELITE should attempt to assess the customer's source of funds to determine whether they derive from illegal activity. This may include querying third party databases, investigating if the customer has sources of wealth/income commensurate with their gaming activity, and ascertaining whether the customer has provided ELITE with identification information or business-related information that can be readily confirmed.

Further due diligence may be warranted if information is obtained indicating the customer:

- Has financial fiduciary duties (e.g., trustee, accountant, attorney, nonprofit/charity executive) that may create a risk of misappropriation or other illicit financial activity;
- Is associated with individuals or entities known to relate to the illicit generation of funds;
- Is a politically exposed person (PEP);
- Claims connections with businesses that have no actual operations; or
- Is the subject of substantial tax liens or has recently gone through bankruptcy.

4. Bank Secrecy Act Compliance

The Bank Secrecy Act (BSA) authorizes the United States Secretary of the Treasury to require financial institutions to file reports and keep records that the Secretary determines to have a high degree of usefulness in criminal, tax, and regulatory matters. The Secretary has designated certain wagering entities as "financial institutions" for purposes of the BSA and has imposed reporting and record keeping requirements on these entities. Whenever these entities facilitate cash transactions with customers that exceed a specified amount, the entities must follow specific federal regulations. ELITE may be required by federal law to comply with the requirements set forth in the BSA. These requirements mandate that employees in the gaming sector be trained in the detection and reporting of suspicious currency transactions. ELITE has instituted such training and emphasizes strict compliance with the BSA in all aspects of its operation. The compliance program is overseen by ELITE's MLRO in concert with ELITE's management, each of whom shares in the responsibility of maintaining ELITE's strict compliance with BSA guidelines.

4.1 Currency Transaction Reporting

To combat potential money laundering risks, under no circumstances will ELITE accept any customer transaction involving either cash in or cash out in any amount.

4.2 Suspicious Activity Reports

Any suspicious transaction relevant to a possible violation of law or regulation will be reported by ELITE to the Department of Treasury on a SAR within 30 days of the transaction date. A SAR is required for suspicious transactions of \$5,000 or more (either a single or aggregated

transaction). The customer involved in the suspicious transaction will not be notified that a SAR has been filed.

5. Government Request for Information and Information Sharing

5.1 Responding to National Security Letters

National Security Letters (“NSL”) are written investigative demands that may be issued by the local Federal Bureau of Investigation and other federal government authorities conducting counterintelligence and counterterrorism investigations to obtain, among other things, financial records of money services businesses. **NSLs are highly confidential. No officer, employee, or agent of ELITE can disclose to any person that a government authority or the FBI has sought or obtained access to records.**

ELITE’s management is responsible for appropriate handling of all NSLs received from the Federal Bureau of Investigation or other federal government authority conducting counterintelligence and counterterrorism investigations.

5.2 Responding to Grand Jury Subpoenas

The receipt of a grand jury subpoena concerning a customer does not in itself require that ELITE file a SAR. When ELITE receives a grand jury subpoena, ELITE will conduct a risk assessment of the customer subject to the subpoena as well as review the customer’s account activity. If ELITE uncovers suspicious activity during its risk assessment and review, it will elevate that customer’s risk assessment and file a SAR in accordance with the SAR filing requirements. ELITE understands that none of its officers, employees or agents may directly or indirectly disclose to the person who is the subject of the subpoena its existence, its contents, or the information ELITE used to respond to it. To maintain the confidentiality of any grand jury subpoena ELITE receives, ELITE will process and maintain the subpoena by:

- Immediately forwarding the request to ELITE’s management to coordinate ELITE’s response; and
- Limiting the dissemination of any grand jury subpoena received on a strict “need to know” basis in order to limit the possibilities the confidentiality requirement being jeopardized.

If ELITE files a SAR after receiving a grand jury subpoena, the SAR will not contain any reference to the receipt or existence of the subpoena. The SAR will only contain detailed information about the facts and circumstances of the detected suspicious activity.

5.3 Sharing of Information with other Financial Institutions Under PATRIOT Act Section 314(b)

Where permitted by law, ELITE may share information about customers suspected of terrorist financing and money laundering with other financial institutions so that these institutions can identify said customers when determining whether to engage in business with them. **ELITE may only share information with other financial institutions that are required to implement an AML program, and this procedure cannot be used to share information about customers suspected of non-criminal financial activity, nor may information be shared once a SAR has been filed.**

If ELITE shares information with another financial institution, it must file with FinCEN an initial notice before any sharing occurs, as well as annual notices thereafter. Before sharing information with another financial institution, ELITE's management must take reasonable steps to verify the other financial institution has submitted the requisite notice to FinCEN, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions that FinCEN will make available.

6. Office of Foreign Assets Control (OFAC)

6.1 Overview

The United States Department of the Treasury's Office of Foreign Assets Control administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. Following sufficient notification, OFAC's regulations require companies to block accounts, payments, or transfers in which an OFAC-targeted country, entity, or individual has any interest. A corresponding report must be filed with OFAC within 10 business days of blocking the relevant account, payment, or transfer.

6.2 What Elite Must Do

OFAC maintains and publishes a list of individuals and companies owned or controlled by, or acting on behalf of, targeted countries. It also lists individuals, groups, and entities such as terrorists and narcotics traffickers, under programs that are not country specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs."

ELITE is required to block transactions involving any SDN on the SDN List and to report the blocked property and/or rejected transaction to OFAC within 10 days.

7. Elite's Operating Procedures

7.1 Account Opening Procedures

Prospective account holders must be introduced or referred to ELITE's management by an existing account holder or a known reliable source. Prospective account holders must submit the following to ELITE's management before an application for a wagering account can be reviewed and potentially approved:

- Government issued ID (valid passport or driver's license)
- Brief biography
- Due diligence background check performed by ELITE's U.S.-licensed private investigator
- Signed Wagering Account Application
- Signed Terms & Conditions Agreement
- Signed Rules & Regulations Agreement

7.2 Account Funding Procedures

Prospective account holders must send funds to ELITE via wire transfer or through personal check deposit for the purpose of opening a new wagering account. The funds must come from

the personal account of the prospective account holder and are traced by ELITE's management to verify compliance. All incoming funds are held in ELITE's accounts at Wells Fargo Bank (U.S.). No cash transactions are allowed at any time, and any deviation from the procedures outlined in this Section 8.2 will disqualify the prospective account holder.

7.3 Account Withdrawal Procedures

If approved for a wagering account, each account holder is assigned a unique TRA code. The TRA code is used by ELITE's management to monitor account holders' wagering activity for suspicious behavior. Requests to withdraw funds from a wagering account will only be considered if sent directly to ELITE's management by the applicable account holder through a verified email address or other authorized messaging service. If the withdrawal request is duly received and verified, a bank wire can be organized by ELITE's management and forwarded directly to the account holder's verified personal account. Control over, and access to, ELITE's bank funds is restricted to ELITE's management and ownership.

Enforcement of the procedures outline in this Section 7 is the responsibility of ELITE's management. Strict adherence to these policies is required, and any deviation from their terms, or any other suspicious activity, will be reported immediately by ELITE's management to the appropriate authorities.