INTERNATIONAL ENTERTAINMENT CORPORATION
國際娛樂有限公司

(Incorporated in the Cayman Islands with limited liability)

(Stock Code: 01009)

SUPPLEMENTAL ANNOUNCEMENT IN RELATION TO THE ENTERING INTO OF THE COOPERATION AGREEMENT; AND COMMENCEMENT OF ONLINE GAMING BUSINESS

Reference is made to the announcement (the "**Announcement**") of International Entertainment Corporation (the "**Company**") dated 9 June 2026 in relation to (i) the entering into of the Cooperation Agreement; and (ii) commencement of Online Gaming business. Unless the context otherwise requires, capitalised terms used herein shall have the same meanings as those defined in the Announcement.

The Board would like to provide additional information on the Online Gaming activities operated or to be operated by the Group as follows:

TYPES OF GAMBLING ACTIVITIES OPERATED AND TO BE OPERATED UNDER THE COOPERATION

According to NCLI's Online Gaming License applied pursuant to the Regulatory Framework for the Accreditation of Gaming System Administrators (the "**Regulatory Framework**") and issued by the Electronic Gaming Licensing Department ("**EGLD**") of PAGCOR, NCLI was accredited as a Gaming System Administrator ("**GSA**") to undertake electronic gaming operations under the following categories: (1) Electronic Casino Games; (2) Electronic Bingo Games; (3) Online Poker Games; and (4) Specialty Games.

At the initial stage of the Online Gaming operations, the Cooperation will focus on Electronic Casino Games, comprising: (i) Electronic Games, which are games of chance where outcomes are generated by a certified Random Number Generator (RNG); (ii) Table Games, being traditional casino games ordinarily played with a dealer but delivered in electronic or online visual format; and (iii) Arcade Games (Specialty Games), which are non-traditional electronic games featuring simple mechanics and entertainment or skill-based gameplay. All the above-mentioned games have been approved and accredited by PAGCOR. These game categories are run through computer-based software, which has been approved by PAGCOR, and do not involve any live human dealers. All these games are operated strictly in accordance with PAGCOR's applicable technical, operational, and regulatory requirements. As of the date of this announcement, the game offerings are still undergoing their trial run. NCLI and TGXI are in the process of refining the operating procedures to address the internal control deficiencies identified in the internal control report. It is expected that these games will commence operations in or about late August or September 2026.

The Cooperation conducts Electronic Casino Games through electronic gaming systems, which are secure, computer-based software platforms that host digital versions of traditional casino games. NCLI is the owner of the Online Gaming Platform ("**OGP**"), while TGXI provides the computer-based software and gaming content supporting the game offerings available on the OGP. In essence, TGXI owns and/or controls the underlying assets, namely the computer-based software, used for the provision, aggregation, integration, and operation of the relevant game offerings. The Cooperation has not yet commenced commercial operations for Electronic Bingo Games, Online Poker Games, or Specialty Games, which are intended to be operated through remote gaming systems. The Group will make further announcements as and when the remote gaming system becomes operational.

The Cooperation does not involve any online gaming services of Integrated Resorts ("**IRs**") that offer land-based casino games through online platforms at this moment. At the current stage, the Group is focused on the development and operation of computer-based online games. The Group intends to expand into land-based electronic gaming terminals in the next phase, including Online Table Games ("**OTG**") and Online Slot Machines ("**OSM**"). The Group will make further announcements as and when it commences the development and deployment of OTG and OSM. NCLI has obtained the provisional licenses for the IR gaming operation. In addition, NCLI has secured all necessary online gaming licenses, certificates of accreditation and approvals for its Online Gaming as follows:

(i) Certificate of Accreditation as a Gaming System Administrator of PAGCOR-Licensed Gaming Venues for Electronic Bingo Games;

(ii) Certificate of Accreditation as a Gaming System Administrator of PAGCOR-Licensed Gaming Venues for Online Poker Games;

(iii) Certificate of Accreditation as a Gaming System Administrator of PAGCOR-Licensed Gaming Venues for Specialty Games;

(iv) Certificate of Accreditation as a Game Content Provider;

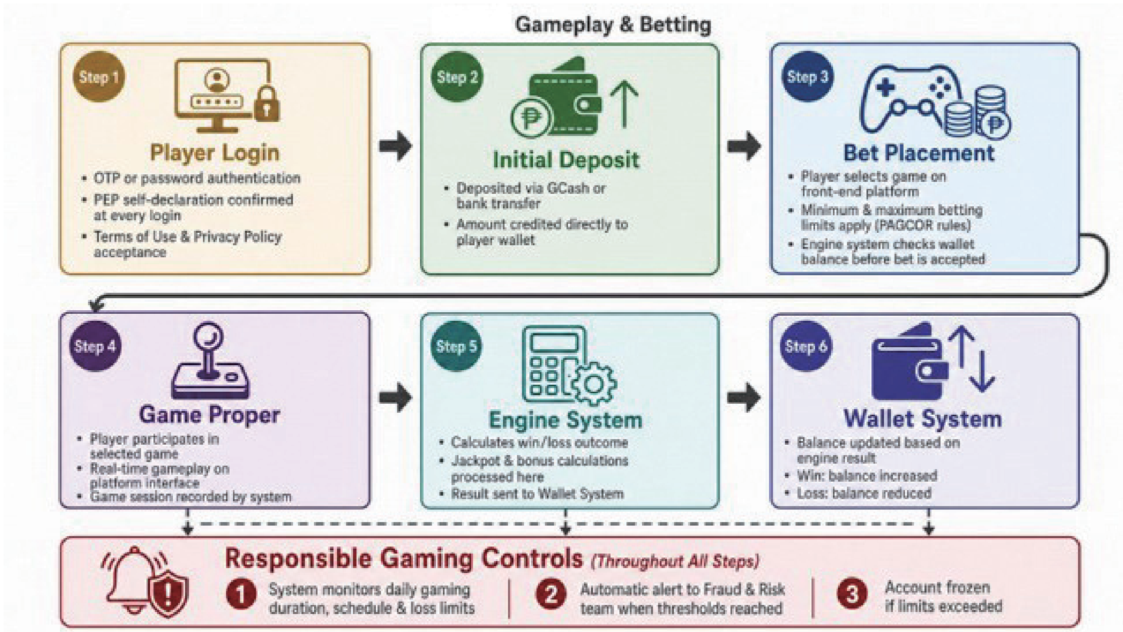
(v) Gaming License as an Electronic Games Operator;

(vi) Notice to Commence (Online Slot Machines); and

(vii) Letter Approval from PAGCOR for the Operation of Online Table Games.

Save as disclosed above, no additional license is required to be obtained before its IR offering OTG and/or OSM.

The following diagram illustrates the operational framework of Electronic Casino Games activities conducted under the Cooperation.



FURTHER DETAILS OF THE APPLICABLE LAWS AND REGULATIONS RELATING TO THE ONLINE GAMING BUSINESS, INCLUDING HOW SUCH LAWS AND REGULATIONS ARE ADMINISTERED AND ENFORCED

The foundational legal instrument for gambling regulation in the Philippines is Presidential Decree (PD) No. 1869, which created PAGCOR and vested it with authority to "*regulate, operate, authorize, and license games of chance, card games, and number games*" within the Philippines.

PAGCOR is the primary regulator for domestic online gambling. Its mandate includes (1) Licensing and regulating internet-based casinos, e-Games, e-Bingo, Online Poker, Specialty Games, and other digital gaming services; (2) Evaluating and approving electronic gaming platforms and systems; and (3) Issuing Gaming Licenses (GLs) for each game category. All domestic-facing online gambling (i.e., platforms serving Filipino players) remains legal and is regulated by PAGCOR. EGLD specifically regulates Electronic Casino (eCasino) Games, Electronic Bingo (eBingo), Online Poker, Specialty Games, Sports Betting, and Numeric Games.

PAGCOR enforces its regulatory powers through five major mechanisms:

Licensing audits: PAGCOR conducts regular audits of licensed operators to verify compliance with technical, financial, and operational standards. These audits include reviews of (i) financial records, (ii) technical system integrity, (iii) responsible gaming measures and AML/Know-Your-Client ("**KYC**") protocols. This is explicitly described as part of PAGCOR's enforcement function.

Law enforcement coordination: PAGCOR works closely with Philippine National Police-Anti-Cybercrime Group, the Department of Information and Communications Technology, through its Cybercrime Investigation and Coordinating Center, and National Bureau of Investigation (NBI) to identify and shut down illegal gambling operations. This includes takedown of illegal online gaming platforms, raids, arrests, imposition of fines and penalties, and seizure of equipment used by unlicensed operators.

AML enforcement: Under RA 10927, online casinos are classified as *covered persons* under the Anti-Money Laundering Act. PAGCOR enforces AML compliance by requiring customer identification, record-keeping of high-value transactions and suspicious transaction reporting. AMLC may freeze accounts or seize assets linked to illicit gambling activity.

Technical oversight: PAGCOR requires operators to use certified RNGs, approved gaming software and secure systems with audit trails. It also mandates real-time system access for monitoring online gaming operations. This is part of PAGCOR's broader regulatory mandate over internet-based casinos and gaming systems.

Administrative sanctions: For any violations of gaming laws, non-compliance with PAGCOR's regulations or breach of the terms and conditions of the license granted by PAGCOR, PAGCOR may impose administrative fines, suspension of operations or cancellation of licenses. This enforcement authority is supported by PD 1602, which penalizes illegal gambling activities not covered by any other specific law.

Regulatory Framework for the Accreditation of Gaming System Administrators: To regulate and govern online gaming operations in the Philippines, EGLD has issued the Regulatory Framework for the Accreditation of Gaming System Administrators. This framework prescribes the accreditation requirements, operational standards, and compliance obligations applicable to GSAs engaged in the management and operation of electronic gaming systems. GSAs accredited by PAGCOR are authorized to undertake electronic gaming operations under the following categories: (1) Electronic Casino Games; (2) Electronic Bingo Games; (3) Online Poker Games; and (4) Specialty Games. Each category requires separate system approval and certification to ensure compliance with PAGCOR's technical, security, and responsible gaming standards. Accredited GSAs must be duly incorporated under Philippine law, demonstrate financial capability, and maintain systems certified for integrity and fairness, including certified random number generators and secure gaming platforms. They are further required to implement responsible gaming measures, comply with anti-money-laundering and data protection regulations, and submit periodic operational and compliance reports to PAGCOR. As to the relevant financial capability, NCLI is required to demonstrate that (1) it has an authorized capital stock of at least One Hundred Million Pesos (PhP 100 Million) of which at least Twenty-Five Million Pesos (PhP 25 Million) must be paid up; (2) it has paid a non-refundable accreditation fee for each game offering in the amount of Five Million Pesos (PhP 5 Million); and (3) it has posted to PAGCOR the required Performance Cash Deposit ("**PCD**") in respect of (a) One game offering with PCD of Twenty-Five Million Pesos (PhP 25 Million); and (b) two or more game offerings with PCD of Fifty Million Pesos (PhP 50 Million). All these financial requirements have been met before PAGCOR issued an Accreditation License to NCLI.

PAGCOR, through the EGLD, exercises regulatory oversight by conducting audits, inspections, and continuous monitoring of gaming systems. It may suspend or revoke accreditation in the event of non-compliance or violations of applicable laws, regulations, or licensing conditions. The framework aims to promote transparency, integrity, and accountability in the conduct of electronic gaming operations, safeguard player interests, and support the Philippine government's objectives for responsible and sustainable gaming development.

With respect to the online gaming services of IR offering land-based casino games through online platforms, the following minimum technical requirements and operational standards shall strictly apply: (a) an IR may only offer its casino table games and slot machines for online gaming through video streaming; (b) an IR may not provide online access to more than twenty-five percent (25%) of its GLDD-approved maximum allowable number of gaming tables, slot machines, or electronic table games, unless a different percentage is expressly approved by PAGCOR through the Gaming Licensing and Development Department ("**GLDD**"); (c) only registered members of the IR may access its approved online gaming platform ("**OGP**"); (d) the OGP must comply with all applicable guidelines and system requirements prescribed under the Regulatory Framework; (e) the OGP must be integrated with PAGCOR's third-party audit platform for online gaming; and (f) all applications for OGP approval by an IR Licensee shall be processed and evaluated by the EGLD.

Anti-Pogo Act of 2025

R.A. 12312, also known as the Anti-Pogo Act of 2025, prohibits the establishment, operation, or conduct of offshore gaming in the Philippines. R.A. 12312 defines offshore gaming as offering or participating in online games of chance or sporting events via the internet using a network and software or program operating in the Philippines, including special economic, freeport, and tourism infrastructure and enterprise zones, catered to offshore players.

In full compliance with the Anti-Pogo Act, NCLI's online gaming operations are exclusively intended for the domestic Philippine market and are accessible only to players who are physically located within the territorial jurisdiction of the Philippines at the time of play.

Foreign nationals and tourists may participate in NCLI's online gaming offerings, provided that they are physically present within the Philippines when accessing and playing the games and that they comply with all applicable registration, identity verification, age-verification, KYC, AML, and other regulatory requirements. Accordingly, the relevant consideration is not the nationality of the player, but the player's physical location at the time of play. Foreign nationals and tourists who are physically present within the territorial jurisdiction of the Philippines may participate in lawful online gaming activities offered by a duly licensed Philippine operator, provided that the gaming activities remain confined within the Philippines and are conducted in accordance with applicable Philippine laws and PAGCOR regulations.

As part of NCLI's registration and KYC procedures, foreign nationals are required to submit valid identification documents, including their passport and, when applicable, their Alien Certificate of Registration, for purposes of verifying their identity and eligibility to register and participate in the online gaming platform.

The registration of a player does not occur automatically even when foreign players residing in the Philippines have submitted all required information. As an additional layer of protection, players identified as foreign nationals are subject to mandatory name screening through a third-party screening service provider, such as Dow Jones. This screening includes, among others, checks against politically exposed persons ("**PEP**") databases, sanctions and watchlists, adverse media reports, related parties, associated entities, and other relevant risk indicators. The AML Team has access to and utilizes the screening solutions for purposes of conducting the relevant screening checks. The Group's Online Gaming business has implemented a three-fold screening process covering the National Data Restriction Program ("**NDRP**"), PAGCOR Exclusion List, and Dow Jones screening solutions. The Group's Online Gaming business has implemented screening against the NDRP and PAGCOR Exclusion List, which also captures persons subject to applicable PAGCOR exclusion orders, as well as screening through the Dow Jones screening solutions. Screening against the NDRP is a function of the existing system and is, therefore, conducted automatically through the system. Screening through the Dow Jones screening solutions is likewise fully implemented, but is currently conducted manually as part of the Group's existing KYC and compliance procedures. Accordingly, all components of the screening process are currently operational and implemented. The existing screening process is compliant with the applicable rules and regulations of PAGCOR, and there is presently no outstanding regulatory requirement requiring the Dow Jones screening solutions to be integrated into the back-end system functionality of the Online Gaming Platform. However, if PAGCOR and/or any other competent regulatory authority subsequently requires the integration of the Dow Jones screening solutions into the back-end system functionality of the Online Gaming Platform, the Group will undertake the necessary system enhancement and implementation in accordance with the applicable regulatory requirements and prescribed timeline.

If a player (whether foreign or local) is identified as being listed in the NDRP, including any sanctions issued by the Philippine government, or appears on the PAGCOR Exclusion List, the system shall automatically reject the player's registration or immediately suspend or restrict the player's account or access to the Online Gaming Platform, as applicable. If a player (whether foreign or local) is flagged through Dow Jones screening, the AML Team shall escalate the case to the Fraud and Risk Department ("**FR Team**") for assessment and appropriate action. Such action may include the suspension of the player's account or the rejection of the player's registration, as applicable. These measures are designed to identify and mitigate potential AML, sanctions, reputational, and other compliance risks. Further, the KYC Team is authorized to review the passports and visas of foreign nationals and to determine whether such individuals qualify to access the online games provided by TGXI, in compliance with Philippine laws and, where applicable, the laws and regulations governing NCLI. If any suspicious circumstance arises, or as may be directed by any competent regulatory authority, NCLI may reject or otherwise deny such player access to the Online Gaming Platform, in accordance with applicable laws, regulations, and internal compliance procedures.

In accordance with the Regulatory Framework for the Accreditation of Gaming System Administrators, all electronic funding and withdrawal transactions involving online gaming platform accounts must be coursed through AMLC-compliant channels. These channels may include over-the-counter and online banking facilities, payment or electronic wallet systems, and other legitimate money transfer services. Only payment systems and money transfer services that are duly accredited, approved, or registered with the Bangko Sentral ng Pilipinas may be used for such purposes.

NCLI's online gaming platform also employs IP-based geolocation and blocking controls, as required by PAGCOR, to restrict access only to players physically located within the Philippines and prevent access from prohibited jurisdictions.

For clarity, although tourists and foreign nationals may engage in online gaming when they are within the territorial jurisdiction of the Philippines at the time of play, they are strictly prohibited from accessing or playing the games when they are outside the Philippines.

THE ONGOING COMPLIANCE WITH EACH OF THE APPLICABLE LAWS AND REGULATIONS

To ensure ongoing compliance with all applicable laws, regulations, and licensing conditions, NCLI has established a dedicated legal and regulatory compliance function responsible for overseeing all matters relating to its Online Gaming Licence and for maintaining continuous communication with PAGCOR. This legal team serves as the primary liaison with PAGCOR on all regulatory submissions, clarifications, and approvals required under the Regulatory Framework and the Manual. In parallel, NCLI has formed a revenue audit team tasked with monitoring, reconciling, and validating all gaming revenues and tax obligations payable to PAGCOR on a daily basis, thereby ensuring full and timely compliance with PAGCOR's financial reporting and remittance requirements.

In accordance with the regulatory framework issued by EGLD, the Cooperation has implemented comprehensive internal controls, technical safeguards, and operational protocols to ensure that the online gaming activities conducted under the Cooperation are secure, transparent, and fully compliant with applicable requirements. These measures include the deployment of PAGCOR-approved gaming systems, the maintenance of tamper-proof audit logs, and the establishment of stringent access-control mechanisms and segregation-of-duties arrangements. The Cooperation also ensures that all system updates, new game deployments, and material modifications to the gaming platform are submitted to PAGCOR for prior review and approval.

To support PAGCOR's supervisory mandate and for compliance purposes, NCLI, being a GSA, ensures that the backend server is directly and continuously accessible to PAGCOR. This connectivity enables PAGCOR to conduct real-time monitoring of gaming transactions, system performance, and compliance with applicable rules and regulations. Such direct access enhances transparency and allows PAGCOR to verify revenue reporting, system integrity, and adherence to responsible gaming, AML, and technical standards at any time.

NCLI, with the operational support, technical assistance, and guidance of TGXI, shall implement the following measures in furtherance of NCLI's continuing compliance obligations:

1. Platform Product Center and Site Reliability Department shall jointly ensure that no online gaming activity, gaming vertical, game content, system, platform, or operational arrangement is launched, modified, or expanded unless the required PAGCOR approval, accreditation, or authorization has first been secured;

2. Site Reliability Department, AML Compliance Team and Information Technology Department shall jointly ensure that the Group's online gaming platform remains duly approved, certified, and compliant with PAGCOR's technical and operational standards. This includes maintaining the required system certifications, ensuring integration with PAGCOR's third-party audit platform for remote or online gaming, observing all applicable operational limits, and implementing internet protocol or IP-blocking controls, player-location controls, platform restrictions, customer eligibility checks, and other safeguards necessary to prevent player registration and betting activity from outside the Philippines, where required.

3. AML Compliance Team shall maintain active coordination with PAGCOR's monitoring teams, comply with venue and operational requirements, and promptly address any findings, directives, or compliance observations issued by PAGCOR.

4. Finance Department and Internal Audit Department shall jointly maintain proper accounting, revenue recording, reconciliation, and remittance procedures to ensure the timely and accurate payment of all applicable PAGCOR shares, license fees, regulatory fees, performance cash deposits, and other required charges. NCLI likewise maintains auditable records and supporting documentation for all gaming revenues, fees, and remittances.

5. Platform Product Center and Site Reliability Department shall jointly ensure that the electronic gaming system, online gaming platform, game content, gaming terminal, machine, or related system used in its online gaming business remains approved by PAGCOR and compliant with the applicable accreditation conditions. NCLI also maintains documentary proof of required certifications, including notarized disclosures or attestations relating to IP-blocking and any other system control required by PAGCOR.

6. Customer Disputes and Support Department ("**CS Team**"), FR Team and AML Compliance Team shall jointly ensure that all gaming affiliates, support service providers, payment gateway providers, marketing service providers, customer service providers, KYC or membership system providers, independent game testing laboratories, and other gaming-related third-party providers are properly accredited or authorized, where required. NCLI shall conduct due diligence on such service providers, incorporate compliance obligations in its contracts, monitor their performance, and require continuing compliance with PAGCOR rules and applicable laws.

7. AML Compliance Team and Internal Audit Department shall jointly maintain an internal compliance monitoring and escalation system designed to prevent, detect, report, and remediate any violation of PAGCOR rules. This should include periodic internal audits, compliance testing, incident reporting, corrective action plans, training of relevant personnel, and prompt reporting or coordination with PAGCOR where required. NCLI shall also maintain a sanctions and accountability framework for internal breaches or operational lapses.

8. Human Resources Department, FR Team, and CS Team shall jointly ensure all personnel required to hold a Gaming Employment License ("**GEL**") maintain valid and subsisting GELs throughout their employment and implement pre-employment

screening, periodic GEL validation, renewal tracking, and employee compliance monitoring, and do not allow any person to perform covered gaming functions without the required valid authorization.

GEL is an authorization issued by PAGCOR granting a person the privilege to be employed as a gaming employee within the Philippines jurisdiction. It is a pre-employment and continuing requirement for employment in any gaming establishment in the Philippines and should form part of the employee's handbook. No employer operating a gaming facility shall hire and keep an individual employed without a valid GEL. PAGCOR conducts periodic GEL compliance verification on all licensees. According to the Legal Opinion, the following personnel must apply for GEL before employment:

(a) Regular or contractual employees hired by the employer, outsourced personnel or those hired through employment agencies whose services are shared between gaming and non-gaming operations;

(b) Outsourced personnel or those hired through employment agencies whose tasks/functions require handling of or direct contact with gaming equipment, paraphernalia, casino cash, chips, tokens, such as, but not limited to dealers, slot machine technicians, slot machine attendants, cashiers, bingo ticket sellers, callers, gaming assistants, etc.; and

(c) Consultants who have participation and/or involvement in the gaming operations.

9. FR Team, CS Team and Site Reliability Department shall jointly implement responsible gaming safeguards, including age-gating, exclusion of minors and prohibited persons, KYC verification, account restriction mechanisms, self-exclusion and voluntary exclusion procedures, betting limits, loss limits, time limits, responsible gaming notices, and customer support channels for gaming-related concerns. These measures should be system-enforced, periodically reviewed, and aligned with PAGCOR's responsible gaming requirements.

   As far as PAGCOR is concerned, gaming licensees or operators may develop their own internal rules and policies relating to membership including but not limited to the registration of gaming members. Under the PAGCOR charter, the following three classes of persons are prohibited from entering, staying, and/or engaging in gaming: (i) government officials connected directly with the operations of the government or any of its agencies; (ii) members of the Armed Forces of the Philippines, including the Army, Navy, Air Force, or the Philippine National Police; and (iii) persons under 21 years of age or students of any school, college, or university in the Philippines.

10. AML Compliance Team shall maintain a robust AML compliance program. This includes customer identification and KYC procedures, enhanced due diligence for higher-risk customers, ongoing transaction monitoring, detection of suspicious and covered transactions, maintenance of transaction records for at least five (5) years, and timely submission of covered transaction reports and suspicious transaction reports to the AMLC within the prescribed period. NCLI shall also ensure that its AML policies, internal controls, and training programs remain updated and aligned with AMLC requirements.

11. AML Compliance Team shall maintain a continuing legal and regulatory monitoring process to address changes in PAGCOR regulations, AMLC rules, data privacy requirements, responsible gaming standards, payment-related rules, tax requirements, and other applicable laws. Since the implementation and interpretation of gaming laws and regulations remain subject to PAGCOR and other competent administrative agencies, and may evolve over time, internal coordination with regulators is maintained on an ongoing basis, with internal policies updated as necessary and periodic compliance reviews conducted to ensure that the online gaming operations remain fully compliant throughout all stages of activity.

NCLI, being the GSA, bears full responsibility for implementing and maintaining all internal control measures governing the Online Gaming operations. Daily monitoring of the internal control procedures, however, is undertaken by the abovementioned departments and/or teams. These departments and/or teams shall prioritise preventive measures over corrective measures to ensure continuous compliance with all applicable laws and regulatory requirements. In addition, NCLI will engage an independent professional to review the internal controls of the operation at least once a year to ensure full compliance.

Upon the identification of any AML red flag or internal control deficiency, the relevant team shall immediately report the matter to the responsible persons of both TGXI and NCLI through the designated software system. TGXI and NCLI shall convene an urgent meeting to assess the issue and determine the appropriate handling measures, including the implementation of any necessary remedial actions. The responsible person of NCLI shall, on the same day, report the issue to the relevant PAGCOR officer. NCLI shall further inform PAGCOR of the remedial actions taken or to be taken to rectify and strengthen the affected internal control procedures.

Accordingly, NCLI's ongoing compliance will be ensured through a combination of prior regulatory approval, continuous license maintenance, platform certification, technical controls, payment and revenue controls, KYC and AML monitoring, responsible gaming safeguards, personnel licensing, third-party oversight, internal audits, record keeping, regulatory reporting, and active monitoring of changes in applicable law and regulatory interpretation.

THE INTERNAL CONTROLS IMPLEMENTED TO ENSURE COMPLIANCE OF ITS ONLINE GAMBLING BUSINESS WITH EACH OF THE APPLICABLE LAWS AND REGULATIONS

To ensure ongoing compliance with applicable laws, regulations, and PAGCOR licensing conditions, the Group has implemented a structured internal control framework supported by dedicated compliance, risk, IT, and revenue-audit functions. These functions collectively oversee game onboarding, system integrity, AML compliance, responsible gaming, data governance, and reporting obligations. The Group's legal department and AML department will jointly be responsible for the identification of any regulatory development.

Game onboarding & integration

Before the game can be integrated into the system, TGXI, as a gaming content provider, should ensure the following: GLI certification is verified; Gaming Operations must check and ensure that the Game to be integrated in the platform has a GLI certification which is obtained by TGXI as Game Provider. Once they receive the certificates, the IT team would obtain the technical integration prerequisites Application Programming Interface ("**API**") procedures, whitelist, and keys to integrate the games into the platform.

Before the game can be integrated into the OGP, the game is submitted to PAGCOR for assessment of its raw data to ensure compliance with local regulations, including an audit of the raw data on the user acceptance testing system.

If the audit is successful, gaming operations must obtain the approval from PAGCOR, accompanied by a certificate. The game is then allowed to be released and integrated. After the game has been allowed to be integrated on the platform by PAGCOR, the business units can now select the newly added game from the approved list on the platform. Once the games chosen are set, the players can view the game and make bets from front-end websites.

Ongoing Monitoring

All licensed game operators are subject to continuous regulatory oversight by PAGCOR throughout the validity of their license. Monitoring is conducted through: (1) Periodic compliance reporting and documentary submissions as required by PAGCOR; (2) Regular audits, inspections, and system reviews etc.; (3) License renewal processes, which require updated submissions and revalidation of compliance with prevailing laws, rules, and PAGCOR regulations; and (4) Immediate reporting obligations. Game operators monitor all licenses, permits, accreditations, and keep them valid and updated at all times, and any lapses or non-compliance may result in regulatory sanctions in accordance with the applicable PAGCOR rules.

Monitoring of win rate of games by PAGCOR

Each gaming platform regularly monitors its key performance indicators, including turnover, gross gaming revenue, and win rates, on a monthly basis as part of its ongoing operational and compliance oversight. The house gain or win rate for each game is fixed based on the game offering approved by PAGCOR during the application of the Online Gaming Licence. Accordingly, NCLI does not have the ability to arbitrarily adjust or manipulate win rates, whether during normal operations or during peak periods such as holidays or festival seasons. Any change to the approved win rate would require prior approval from PAGCOR before implementation.

Daily Gaming Activity & Reporting

Gaming transaction data flows from the front-end interface to the game engine and is transmitted in real time to the backend data centre, where records are retained for three months before deletion. The data is then transferred to the long-term data lake for storage and analytical use. All servers and databases are hosted in two separate cloud storage locations, ensuring redundancy and enabling rapid recovery in the event of a system failure.

Daily wager/bet amounts are stored in the "Data Lake". These data are pooled in for the purpose of daily recording of transactions by the back office and for audit performed by the external third party (the "**PAGCOR Contractor**") that specializes in IT and data audit, who performs audit on behalf of PAGCOR. Gross Gaming Revenue reports are extracted from the "Data Lake" in which PAGCOR Contractor can also access. This is used for daily revenue checking and weekly revenue reporting of the back office. The data from "Data Lake" is also used by business units for the game popularity evaluation. The revenue reporting team uses data from the back office to check the revenue reasonableness. The data in the "Data Lake" is processed by the back office (Revenue Reporting) where a Gross Game Report (GGR) is prepared. The GGR incorporates all transaction data pulled from the data centre and is prepared for the weekly audit of the PAGCOR Contractor, which also pulls the raw data related to GGR to ensure that the report sent to them by the Revenue Reporting team matches the raw data independently pulled out of the "Data Lake". Betting logs are retrieved from the system and reconciled on a monthly basis. The amount will also be reconciled with PAGCOR. The Revenue Reporting Accountant extracts monthly data from the back-office system and records the figures in Business Central upon approval by the Deputy Revenue Head.

Responsible Gaming Regulations and Considerations

Responsible gaming requirements are currently governed by existing PAGCOR regulations, license conditions, and system standards applicable to licensed electronic gaming operators. In particular, PAGCOR regulations expressly require that: "The Electronic Gaming System (EGS) along with its Operator Gaming Platform (OGP) must have a feature allowing the player to set his/her betting limits daily, weekly and/or monthly."

In compliance with responsible gaming requirements, licensed operators are mandated to implement player-controlled betting limit features within their gaming systems as part of PAGCOR's responsible gaming safeguards. In addition to betting limits, responsible gaming measures under existing PAGCOR rules and directives generally include: (1) Player protection and responsible gaming messaging; (2) Mandatory KYC and age verification controls; (3) Self-exclusion and account restriction mechanisms; (4) Monitoring of player activity for responsible gaming indicators. The responsible gaming indicators are "Player daily gaming duration" "player daily gaming schedule" and "player daily loss limits". The Operating Management System ("**OMS**") automatically generates alerts to FR Team when predefined player behavior thresholds are reached. In case of any suspicious transactions, the team would freeze the account from access when the threshold is surpassed.

Online issue handling and system availability

System health alerts are monitored by Gaming Operations. The online issue is detected through customer service team and the monitoring system. The issue would raise a case ticket in the system. Manual checking by Gaming operations when reports are raised by the users of the platform.

Incidents are first reported by players and received through user-support channels, then escalated to the Duty Team for initial handling. Unresolved issues are passed to the Level-2 Engineer and, where required, to the Manager for final resolution. The workflow is governed by established SOPs covering escalation steps, communication protocols, and post-incident review.

The issue is then sent to 24-hour duty team, and the duty team will try to solve the issue within 10 minutes. If it cannot, the issue will be escalated to the engineers. If the issue persists after 20 minutes, the engineers synchronize the information with other teams through Contractor group chat. Last resolution will be escalation to Manager.

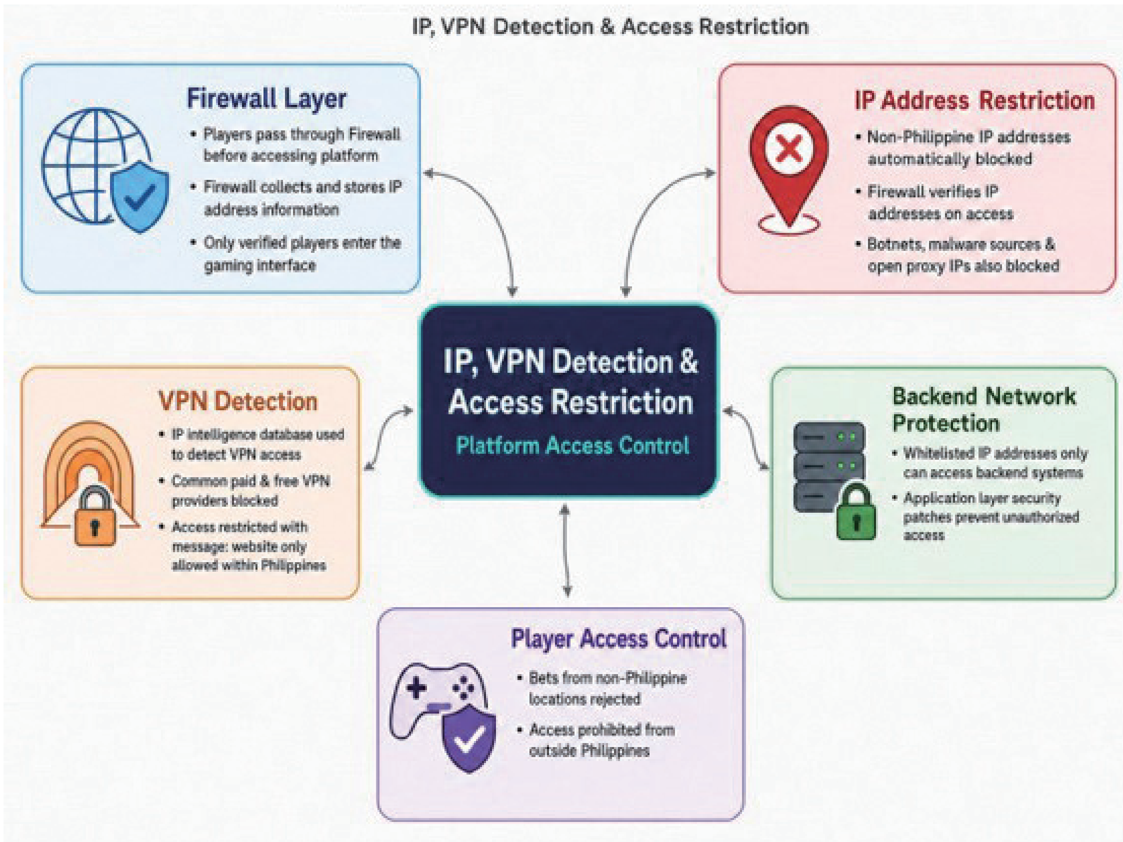
IP, VPN, and Access Restriction Controls

NCLI has implemented a multi-layered access-control and geo-restriction framework to ensure the security of its gaming systems and full compliance with PAGCOR's requirement that only players located within the Philippines may access licensed online gaming platforms. At the network layer, access to NCLI's backend systems is restricted through an IP-whitelisting mechanism, allowing only authorised internal IP addresses to perform system maintenance and operational functions. At the application layer, security patches and code-level protections are applied to prevent unauthorised access and safeguard system integrity.

Before players can access the gaming interface, all traffic is routed through the platform's Content Delivery Network ("**CDN**"), which captures and verifies IP-related information. The Electronic Gaming System ("**EGS**") deployed under the Cooperation is configured to prohibit player registration and betting activity originating from outside the Philippines. To enforce this requirement, the CDN firewall and IP-intelligence tools will automatically block non-Philippine IP addresses and detect attempts to access the platform through virtual private networks ("**VPNs**"). Where VPN-based access is detected, Site Reliability Department and Information Technology Department coordinate with Cloudflare for further investigation and remediation. The effectiveness of these controls has been validated through testing using multiple commercial and free VPN services, all of which were unable to bypass the platform's geo-restriction measures. Users attempting to access the platform from outside the Philippines receive a system-generated notification stating that the website is restricted to users within the Philippines.

In addition to geo-blocking, the Online Gaming systems automatically block IP addresses associated with botnets, malware sources, and known open proxy endpoints commonly used for cyberattacks.

These measures collectively ensure that only eligible players within the Philippines may access NCLI's gaming services, while maintaining robust protection against unauthorised access, cyber threats, and regulatory breaches. The following diagram illustrates IP, VPN, and Access Restriction Controls under the Cooperation.



Anti-Money Laundering (AML)

AML policy update and training

NCLI adopts the State policy under AMLA, and has established a comprehensive Money Laundering and Terrorist Financing Prevention Program ("**MTPP**") to ensure full compliance with all applicable anti-money-laundering and counter-terrorist-financing requirements governing licensed online gaming operators in the Philippines. The MTPP is subject to periodic review and is updated at least once every two years, or earlier when necessary, to reflect amendments to AML/CTF laws, regulatory issuances of the AMLC and PAGCOR, and emerging detection techniques and typologies relevant to electronic gaming operations. AML Compliance Team is responsible for transaction monitoring and due diligence.

Risk and Compliance team is responsible for AML policy update and assessing the impact. As part of its compliance governance, the Risk and Compliance Team conducts daily monitoring of regulatory websites and newly issued guidelines or memoranda. Upon identification of any regulatory development, the Risk and Compliance Team prepares a draft revision assessing the impact of such changes on NCLI's internal policies and procedures. The draft revision is circulated to relevant business units and stakeholders for comment, after which the Risk and Compliance Team finalises the updated MTPP. The revised policy is then submitted to management for approval. Once approved, the updated MTPP is disseminated to employees through email and NCLI's Contractor system to ensure timely implementation across all operational units.

Approval of a policy revision triggers an internal assessment to determine whether additional AML training is required. Where necessary, NCLI conducts targeted or organisation-wide AML training to ensure that employees understand the updated regulatory requirements and are equipped to implement the revised controls effectively. This process ensures that NCLI's AML framework remains current, responsive to regulatory developments, and fully aligned with PAGCOR's licensing conditions and AMLA obligations applicable to online gaming operators in the Philippines.

Transaction Monitoring and Filing Process (including CTR and STR)

In order to identify suspicious transactions in a timely manner and adhere to AMLA and MTPP, the Company employs an automated monitoring framework supported by the system of TGXI (the "**TGXI System**") and the OMS. The TGXI system automatically flags potential suspicious activity based on predefined parameters, including the use of multiple accounts by the same player, the submission of fake or unclear identification documents, deposits without corresponding gaming activity, incomplete KYC information, and attempts by internal employees, who are prohibited from gaming, to access the platform. OMS performs multiple scans throughout the day, depending on player volume, and generates alerts that are routed to the front-end risk team for initial review.

Upon receipt of an alert, the front-end risk team conducts a preliminary assessment and records its findings in OMS. All reviewed transactions, whether AML-related or not, are transmitted to the system, which interfaces with OMS and serves as the primary platform for AML compliance review. The AML Compliance Team examines the exclusion report generated in the system, filters transactions with potential money-laundering indicators, and initiates formal investigation procedures. Each case is documented in the AML compliance form within Contractor, and the investigation includes a review of transaction patterns and KYC information.

Following the completion of the investigation, the AML Compliance Manager prepares a Preliminary Suspicious Transaction Report ("**PSTR**") with recommendations and justification. The PSTR is reviewed by the Head of AML Compliance and subsequently endorsed to the AML Committee, which comprises the Head of Legal, Head of Finance, and Head of Operations. Once approved, the PSTR is elevated to a Suspicious Transaction Report ("**STR**") and filed with the AMLC through the AMLC portal within the statutory reporting period. Customer service personnel are likewise trained to identify suspicious behaviour during customer interactions and may initiate TGXI System workflows that follow the same investigative and reporting process.

In accordance with AMLA requirements, suspicious transactions must be reported within five working days. NCLI's internal timeline provides for a three-day investigation window, allowing sufficient time for internal approvals prior to statutory filing. The TGXI System automatically generates case tickets with countdown indicators to ensure timely closure, and AML Compliance Officers monitor open cases daily to prioritise those nearing the deadline. To comply with AMLA, the AML Compliance Team also performs daily checks of the exclusion report to confirm that all suspicious transactions have been captured and escalated.

Additional alert triggers include unclear identification documents, which are assessed through an external verification tool (Zoho), and matches against government blacklists maintained under the NDRP. The blacklist is regularly updated in OMS based on applicable regulatory lists, PAGCOR directives, the National Database of Restricted Persons, internal exclusion records, self-exclusion records, AML alerts, fraud monitoring results, and other relevant compliance sources. The system is integrated with an API that is synchronized with the NDRP blacklist maintained by PAGCOR. As a result, any newly blacklisted individuals are automatically added to the API and detected by the system during eKYC registration attempts. This automated detection remains effective provided the API connection is operational. Information about a blacklisted customer in the NDRP list from the PAGCOR website is stored electronically and is not automatically removed.

It is the customer's responsibility to contact the customer service team to request removal from the blacklist in order to regain eligibility for registration. Until such action is taken and approved, the customer remains indefinitely banned from registering. However, once an individual is removed from the NDRP blacklist and the API is updated accordingly, that person can immediately proceed with registration. If no other issues are detected during verification, the registration will be approved. When the system process is unavailable (e.g., when API is down), a daily manual check is conducted to update the blacklist in the system, ensuring that the blacklist remains current and accurate. The FR Team logs into the PAGCOR website and retrieves details of newly blacklisted individuals. These individuals are then manually added to PAGCOR Blacklist Compilation list (PBC list), including all details obtained from PAGCOR. The system automatically suspends newly registered players whose names and birthdates match entries in the NDRP database. The system also suspends accounts when a player is identified as blacklisted.

AML assigning risk score to the players/Due diligence

NCLI maintains a comprehensive player-risk assessment and due-diligence framework as part of its obligations under the AMLA and PAGCOR's regulatory requirements. The AML Compliance Team conducts multiple daily reviews of player activity, including identity information, gaming behaviour, and funding patterns, to ensure consistency with each player's established risk profile. In addition to internal monitoring, player information is screened against the Dow Jones solutions and other international adverse-media sources. A risk score is assigned based on screening results, and the corresponding risk level is documented in the player's risk-profiling record. Risk levels are updated when a player engages in high-value transactions, such as bets or withdrawals exceeding PHP 3,000,000 in a single transaction.

NCLI also screens players to identify politically exposed persons ("**PEPs**") and immediate family members and known related entities of the PEPs against the Dow Jones screening solutions. Where a player is identified as a PEP or immediate family members and known related entities of the PEPs, NCLI records the identities of such PEP and/or his/her immediate family members and known related entities by screening against the Dow Jones screening solutions and other international or public sources. NCLI then assesses the heightened risks associated with the PEP's position.

The due-diligence process for online gaming players is guided by a structured AML risk-scoring framework that evaluates each player across behavioural, financial, and profile-related criteria. These include the validity and completeness of identification documents, responsiveness to KYC updates, social status and screening results, source of income, jurisdictional risks associated with employment or business, potential non-gaming use of the gaming account, abrupt changes in betting behaviour, large transactions with minimal gameplay, and the average size of deposits or withdrawals. Each criterion is scored from 1 to 3, with higher scores indicating greater AML exposure. The cumulative score assigns players to one of three risk tiers: Low (1–9 points), Medium (10–18 points), or High (19–27 points).

The assigned risk tier determines the level of Customer Due Diligence (CDD) required. All CDD procedures begin with facial recognition and identification verification through the KYC process, with records maintained in the player's KYC profile within the system. Simplified Customer Due Diligence (SDD) is applied to low-risk players, which includes collecting minimum required information, obtaining valid identification, recording transactions in the system for monitoring, and updating customer information every five years or upon a material change in the customer's profile. Medium-risk customers are subject to Normal Customer Due Diligence (NDD), which includes collecting and verifying required customer information through valid documents and reliable open sources, conducting ongoing monitoring of the customer relationship and transactions, and reviewing the customer profile every three years or upon a material change. High-risk customers are subject to Enhanced Customer Due Diligence (EDD) when there are concerns regarding the accuracy or completeness of customer information, source of funds or wealth, third-party transactions, PEP or adverse information, changes in risk classification, or other suspicious activity indicators. EDD may include obtaining additional information and supporting documents, assessing the source of funds and wealth and purpose of transactions, reviewing historical and ongoing gaming activity for irregular patterns, obtaining AML Committee approval before proceeding with transactions, and conducting semi-annual reviews for customers with substantial activity. For players requiring EDD, NCLI undertakes additional verification measures, which may include gathering supplementary identification documents, reviewing publicly available information, and validating historical and ongoing gaming transactions to identify patterns, trends, or irregularities. In practice, EDD is triggered when a player conducts a transaction exceeding PHP 3,000,000 or when the player appears on the blacklist maintained under the NDRP. These enhanced procedures ensure that NCLI maintains robust oversight of high-risk players and complies with all AMLA and PAGCOR requirements applicable to licensed online gaming operators in the Philippines. If the player fails EDD for a specific transaction or gameplay, the system notifies PAGCOR and the associated funds are forfeited. If the player passes EDD, the account is cleared and allowed to proceed.

AML Training

AML training will be provided to employees who are responsible for implementing NCLI's anti-money-laundering internal controls and procedures. Training programmes are role-based and function-specific to ensure that AML/CFT knowledge is delivered to the appropriate personnel and that employees are equipped to comply with their obligations under the AMLA and PAGCOR's regulatory requirements. A training calendar and roadmap are maintained to ensure that the training needs of relevant employees are addressed in a timely manner.

Training materials are developed in accordance with the operational responsibilities of each department and are reviewed and validated by both the respective department head and the AML Compliance Officer. The materials cover key areas including customer identification and due diligence, the recognition and reporting of covered and suspicious transactions, record-keeping requirements, and other internal control processes. These materials are reviewed and updated annually prior to the conduct of refresher training.

Following each training session, employees are required to complete an examination to assess the effectiveness of the training. Employees who do not achieve a satisfactory result are required to undergo additional training and re-examination until the required standard is met. All training materials, attendance records, and examination results are maintained by the AML Compliance Officer for a period of five years in accordance with regulatory requirements.

THE BOARD'S ASSESSMENT, WITH DETAILED BASIS, ON THE EFFECTIVENESS OF THE INTERNAL CONTROLS IN OVERSEEING THE COMPLIANCE OF ITS ONLINE GAMING OPERATIONS

The management of NCLI has held extensive discussions with the IC Consultant, who was engaged to review the design of the internal control system ("**ICS**") proposed for adoption in connection with the Online Gaming operations under the Cooperation. As part of this review, the IC Consultant conducted interviews and walkthrough testing across key control areas, including KYC procedures, gaming operations, AML controls, customer support processes, and dispute-resolution mechanisms. The IC Consultant identified three areas with medium risk, one area with low risk and one area that requires management improvement. Two of the medium risks are found in KYC process, these include (1) absence of periodic reconciliation for manual blacklist updates and re-screening for new players during API downtime; and (2) automatic approval of previously blacklisted individuals without enhanced review. One medium risk and one management improvement item are relating to AML. In AMLC Regulatory Issuance (ARI) A, B and C, No.3 Series of 2018 — Guidelines on Digitization of Customer Records, Online Gaming operator shall implement the digitization of all customer records that they will henceforth receive, create or open. However, the current policy did not adhere to the digitization standard and stored its customer risk profile offline in paper form to fulfil compliance requirements. One low risk is relating to customer service procedure, in which the IC Consultant considered that there is lacking of system integration for hotline calls and emails and live messages to fulfil the regulatory requirement. As to the management improvement item, the IC Consultant found that the current policy is lacking of procurement requirement of external parties hired in AML process. The IC Consultant has provided corrective action plan and NCLI agreed to adopt and take the relevant action.

Based on the IC Consultant's independent assessment, no significant internal control deficiencies were identified in the ICS to be adopted for the Online Gaming operations. The IC Consultant also provided recommendations to enhance certain control areas, all of which NCLI has confirmed it will adopt and implement as part of the continuous strengthening of its internal control framework. The Company is currently in the process of implementing the recommendations of the IC Consultant and continues to take the necessary follow-up actions to enhance the relevant control areas. The implementation is ongoing, and the Company will continue to work towards completing the applicable recommendations as soon as practicable. It is expected that the enhancement of the internal control will be accomplished in or about late August or September 2026. Thereafter, the IC Consultant will perform further internal control review. As advised by the IC Consultant, the internal control review report is expected to be submitted to the Board in or about December 2026 and the Company will make further announcement to disclose the findings of the IC Consultant's review report accordingly. Having considered the conclusions of the internal control review and the discussions with the IC Consultant, the management of NCLI is satisfied that the Online Gaming operations conducted under the Cooperation, which incorporate the internal control procedures and measures reviewed and recommended by the IC Consultant, are subject to appropriate governance and oversight. Accordingly, the Board is of the view that adequate and effective internal control policies and measures are in place for the Online Gaming operations carried out pursuant to the Cooperation.

THE OPERATING MODEL OF THE GROUP'S ONLINE GAMING BUSINESS, INCLUDING, BUT NOT LIMITED TO, DETAILS OF THE ONLINE PLATFORM, REGISTRATION PROCEDURES, DEPOSITS AND WITHDRAWALS ARRANGEMENTS, AND THE ONGOING MONITORING MECHANISMS FOR USER REGISTRATION AND TRANSACTIONS ON THE PLATFORM

The Online Gaming business under the Cooperation operates through a heavily regulated online gaming platform that is accessible only to users who satisfy the prescribed eligibility, registration, verification, and compliance requirements.

A user may not freely access, deposit, withdraw, or participate in gaming activities without first undergoing the platform's registration and KYC process. The platform is designed to implement front-end preventive controls, such that eligibility is verified prior to access, rather than relying merely on post-activity review or after-the-fact compliance checks.

The registration process begins with the user's access to the online platform, where eligibility notices and disclosures are prominently displayed. These notices identify persons who are prohibited from registering, accessing, or participating in online gaming activities, including minors, government officials, uniformed personnel, persons below twenty-one (21) years of age, persons included in PAGCOR's NDRP, Gaming Employment License holders, and other disqualified persons. The user is required to review and accept the disclosure before proceeding.

Thereafter, the user is required to input his or her mobile number to initiate the registration or log-in process. An automated one-time password ("**OTP**") is then sent to the declared mobile number, and the user must input the correct OTP before proceeding further. This step verifies the user's ownership and control of the declared contact number. Only after completion of these initial steps is the user considered registered; however, registration alone does not confer gameplay access.

Immediately upon registration, the user is required to complete KYC process, which refers to the overall customer identification and due diligence process. The KYC process requires, among others, the submission of a valid government-issued identification document, face verification through facial recognition technology, collection and confirmation of personal information, such as, but not limited to, the residential address, contact details, and source of funds of the player, and final affirmation of the data submitted by the user. These verification layers are system-enforced and are designed to authenticate identity, validate age and eligibility, and prevent impersonation, fraudulent registration, or the creation of accounts by prohibited persons.

During the KYC process, the users are required to complete the KYC verification, which is a specific step within the KYC process involving the verification of customer's identity and submitted information. If the KYC verification is approved, the user will receive confirmation and may continue to access the platform subject to the applicable terms and regulatory controls. If rejected, the user is notified of the reason for rejection and must coordinate with customer support before re-attempting verification. Users who fail to pass the KYC verification are restricted from accessing games on the platform.

With respect to deposits and withdrawals, the platform is structured so that users who have not completed and passed KYC process cannot deposit nor withdraw funds. No deposit nor withdrawal may be processed unless the KYC process has been successfully completed and approved. Further, if a user is identified as a prohibited person, listed in the NDRP, or otherwise disqualified under applicable regulatory rules, the account is automatically denied activation. In such cases, the user is prohibited from accessing games, making deposits, withdrawing funds, or using the platform in any capacity.

The deposit and withdrawal arrangements may include electronic payment channels, including e-wallets, subject to applicable regulatory requirements, verification, transaction monitoring, and reporting obligations. Only duly licensed and accredited payment channels by the *Bangko Sentral ng Pilipinas* (Central Bank) are authorized as payment gateways in the platform. In the regulated setting, the use of such payment rails is intended to support traceability, fraud controls, consumer protection, and compliance monitoring.

NCLI also maintains ongoing monitoring mechanisms throughout the entire user lifecycle. KYC compliance is dynamic and continuous, and does not end upon initial registration. Ongoing monitoring and re-validation procedures may be triggered by inconsistencies in submitted documentation, irregular transaction behavior, device anomalies, multiple account linkages, rapid fund movements, mismatched identity data, repeated failed verification attempts, account behavior suggesting elevated risk, or other system-generated alerts.

The platform is also integrated with controls for prohibited persons and regulatory exclusion lists, including the NDRP. As part of the registration and KYC process, accounts are screened against applicable exclusion databases. If a user is identified as listed in the NDRP or otherwise prohibited, the system triggers immediate restriction, including freezing or denial of account activation. Banned or restricted users are prohibited from accessing games, making deposits, withdrawing funds, or otherwise using the platform.

CS Team and FR Team are responsible for KYC verification. The system automatically performs the identification based on parameters such as multiple accounts of the same player, player using a fake ID, deposit without gaming activity, underage players etc.. After identifying these parameters many times per day, the system will send alerts to front-end risk team whenever a parameter is identified. If any of the information is incomplete or incorrect, FR Team will transfer the case to CS Team, which will then resolve the issue with the user's eKYC submission. After submission to the CS Team, the eKYC status will now be transferred to "Customer Fixing". Once completed, the CS Team will then correct the required information, such as the name, date of birth, ID number, or gender, based on the FR Team documentation. The FR Team will conduct another manual review. If everything is correct, the FR Team will approve the user's eKYC. The above issues may occur and be resolved from time to time.

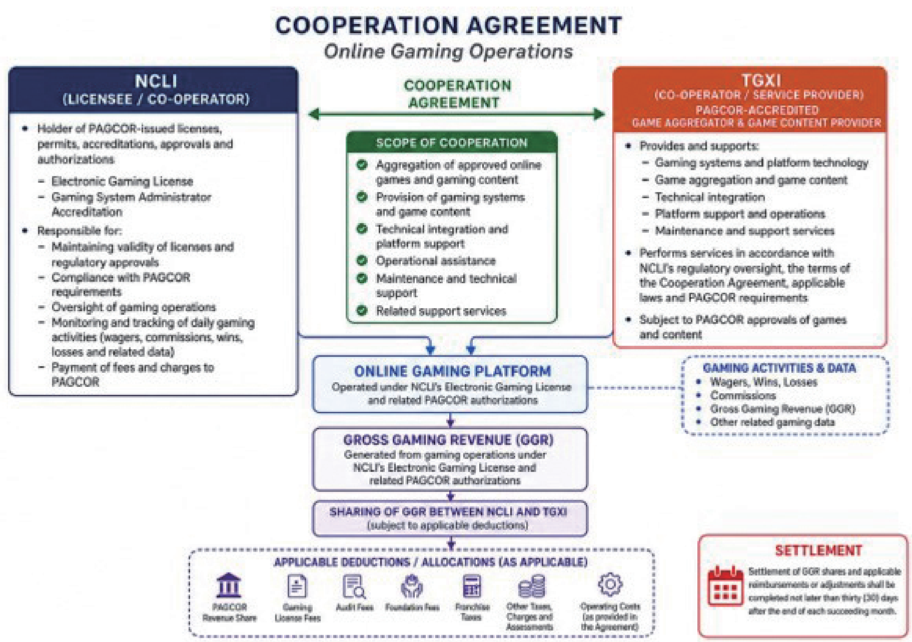
Should the FR Team determine that any of the relevant parameters have been breached, the FR Team will suspend the account, as appropriate. The Compliance Team will thereafter submit to PAGCOR, on a monthly basis, a list of suspended accounts together with the corresponding reasons for suspension. If the circumstances fall within the parameters of a covered transaction or suspicious transaction under applicable anti-money laundering laws and regulations, the AML Team will assess the matter and file the appropriate report with the Anti-Money Laundering Council ("**AMLC**") (i.e., Covered Transaction Report ("**CTR**") or Suspicious Transaction Report ("**STR**")), as may be required.

In addition, NCLI's monitoring framework supports compliance with anti-money laundering, fraud prevention, responsible gaming, and regulatory reporting obligations. Where transactions or account behavior indicate possible fraud, money laundering, identity misrepresentation, account takeover, financial system abuse, or other illicit activity, the matter may be escalated for compliance review and, where warranted, the appropriate regulatory reports, including Suspicious Transaction Reports and other mandated submissions, may be prepared and submitted to the relevant regulators.

NCLI likewise implements responsible gaming safeguards, including account restriction, player banning, mandatory exclusion, voluntary exclusion, self-exclusion mechanisms linked to PAGCOR procedures, and betting, loss, and time limits. These mechanisms are designed to provide both regulator-driven and user-driven safeguards against excessive or unauthorized gaming activity. The system continuously monitors user activity against applicable restrictions and thresholds, and automatically enforces restrictions or generates alerts when risk indicators or limits are triggered.

FURTHER DETAILS OF THE COOPERATION AGREEMENT, INCLUDING, BUT NOT LIMITED TO, THE BUSINESS MODEL, BOOKMAKING ARRANGEMENT, REVENUE AND PROFIT-SHARING ARRANGEMENT, ROLE AND RESPONSIBILITIES OF EACH OF NCLI AND TGXI

The Cooperation Agreement establishes a structured operating model under which NCLI acts as the licensed Online Gaming Operator and GSA, while TGXI functions as the technical service provider, game aggregator, and game content facilitator. The Cooperation delineates regulatory responsibilities to NCLI and technical-operational responsibilities to TGXI, forming a compliant and scalable framework for domestic-facing online gaming operations in the Philippines. The following diagram outlines the business model under the Cooperation.



Business Model of the Cooperation and role and responsibilities of the parties

Under the Cooperation Agreement, NCLI, as the licensee and holder of the relevant PAGCOR-issued licenses, permits, accreditations, approvals and authorizations, engages TGXI, as a PAGCOR-accredited Game Aggregator and Game Content Provider, to provide the necessary support and maintenance for the continued use and operations of the gaming software systems, game aggregation, game content, platform support, technical integration, operational assistance, and related support services required for the operation of approved online games. The cooperation covers the aggregation, provision, integration, and technical support of approved online games and gaming content, subject at all times to applicable laws, PAGCOR requirements, and the terms of the Cooperation Agreement.

The Gaming Operations arrangement is structured to be conducted under NCLI's Electronic Gaming License and Gaming System Administrator Accreditation. NCLI remains responsible for maintaining the validity of the relevant online gaming licenses and permits, ensuring that the online gaming platform and operations comply with applicable PAGCOR requirements, and tracking daily gaming activities, including wagers, commissions, wins, losses, and related gaming data. TGXI's role is primarily to provide the gaming systems, content, aggregation, integration, technical, operational, and support services necessary for the approved online gaming operations.

With respect to the revenue and profit-sharing arrangement, the Cooperation Agreement provides that the revenue source shall be the Gross Gaming Revenues ("**GGR**") derived under the Electronic Gaming License and related PAGCOR authorizations necessary for the operation and use of the online gaming platform. The agreed GGR sharing ratio between NCLI and TGXI is three percent (3%) for NCLI and ninety-seven percent (97%) for TGXI, subject to applicable deductions, including PAGCOR share, gaming license fees, audit fees, foundation fees, franchise taxes, and other applicable taxes and charges. Profit-sharing settlement is required to be made not later than thirty (30) days after the end of each succeeding month.

NCLI's principal roles and responsibilities include:

(i) maintaining the validity of its Electronic Gaming License, Gaming System Administrator Accreditation and other requisite PAGCOR permits, approvals, accreditations, certifications, and authorizations necessary for the operation and use of the OGP;

(ii) complying with the applicable PAGCOR, AMLC, NPC, and other regulatory reportorial and compliance obligations applicable to its license and accreditation;

(iii) notifying TGXI of any notice, order, investigation, suspension, revocation, restriction, show-cause order, compliance finding, or regulatory action that may affect the Cooperation Agreement;

(iv) providing the necessary manpower to accomplish its undertakings under the Cooperation Agreement;

(v) tracking daily gaming activities, performance, and reporting results;

(vi) performing revenue audit to ensure revenue accuracy, completeness, compliance, collecting gaming revenues and remitting TGXI's corresponding share;

(vii) ensuring that online gaming operations are conducted in a PAGCOR-approved venue (i.e. the physical gaming site approved by PAGCOR) or through approved channels (i.e. the PAGCOR-approved URL, website, or online gaming platform through which the relevant online gaming activities are made available); and

(viii) paying, filing, and settling the applicable gaming taxes and regulatory fees, subject to the agreed sharing and reimbursement mechanics under the Cooperation Agreement.

TGXI's principal roles and responsibilities include:

(i) providing the necessary support for the gaming software system, game aggregation, game content, platform support, and related gaming content provider services;

(ii) providing manuals, technical references, APIs, integration documents, operational instructions, game documentation, and other technical support necessary for system integration and operation;

(iii) providing NCLI with access to relevant transaction, game transaction, and operational data reasonably required for regulatory compliance and reporting;

(iv) providing information necessary to assist NCLI with AML-related reporting and transaction tracing; and

(v) maintaining its PAGCOR accreditation, license, authority, or registration as may be required for its activities as Game Aggregator and Game Content Provider.

Book-Making Arrangement

All book-making activities for the Online Gaming operations conducted under the Cooperation take place exclusively within the Philippines. As the licensed operator, NCLI is responsible for the bookmaking arrangement. To ensure that only players physically located in the Philippines may access the gaming platform, the Cooperation has implemented a comprehensive, multi-layered access-control and geo-restriction framework. At the network layer, backend system access is restricted through IP-whitelisting, permitting only authorised internal staff to access operational systems. At the application layer, security patches and code-level protections are applied to prevent unauthorised access.

Before entering the gaming interface, all player traffic is routed through CDN, which captures and verifies IP information. The platform further employs Cloudflare's IP-intelligence and VPN-detection tools to automatically block non-Philippine IP addresses and VPN-based access attempts. In addition, IP addresses associated with botnets, malware sources, and known proxy endpoints are proactively blocked. The effectiveness of these geo-restriction measures has been validated through testing using multiple commercial and free VPN services, all of which were unable to bypass the system's controls. As a result, NCLI confirms that all wagers, bets, and book-making activities originate solely from players located within the Philippines, in full compliance with PAGCOR's regulatory requirements.

Revenue and Profit-Sharing Arrangement

Under the Cooperation, NCLI and TGXI share revenue generated from the Online Gaming operations based on an agreed revenue-sharing mechanism. NCLI, as the licensed operator, is responsible for:

- Performing revenue audits to ensure accuracy and completeness of gaming revenue.
- Verifying data through access to TGXI's collection and payment systems.
- Ensuring prompt distribution of NCLI's revenue share and the advance of gaming taxes.

TGXI provides the necessary transactional and technical data to support NCLI's revenue audit and reporting obligations.

THE REQUIRED PAYMENTS TO BE PAID TO PAGCOR AND THE BUREAU OF INTERNAL REVENUE AS AN ONLINE GAMING OPERATOR

Performance Cash Deposit

As GSA, NCLI shall post to PAGCOR the required Performance Cash Deposit (PCD) before commencing operations. The amount of PCD required will depend on the number of game offerings. For one game offering, the GSA shall pay Twenty-Five Million Pesos (PhP25 Million). Any two or more game offerings, the PCD shall be Fifty Million Pesos (PhP50 Million). NCLI has paid the required PCD to PAGCOR and is eligible to commence its Online Gaming operations accordingly.

Gross Gaming Revenue ("GGR") Sharing

Under the Philippine regulatory framework, a PAGCOR-licensed online gaming operator is required to remit to PAGCOR a prescribed share of its GGR, being the total wagers received from players less the total winnings paid out. This GGR share constitutes PAGCOR's primary regulatory fee and represents the government's participation in the revenues generated from licensed online gaming activities. The applicable GGR share varies depending on the type of game offered, with PAGCOR generally imposing higher rates on electronic casino games and lower rates on online poker and other specialty games. These GGR-based regulatory fees are payable directly to PAGCOR and are distinct from national taxes imposed by the Bureau of Internal Revenue.

License fees

In addition to the GGR share, online gaming operators are required to pay various licensing, accreditation, and monitoring fees to PAGCOR. These include application and annual licence fees, system testing and certification fees, and fees associated with PAGCOR's real-time monitoring of gaming systems and integration with its third-party audit platform. Operators offering games through Electronic Gaming Sites may also be subject to site accreditation fees, terminal approval fees, and annual renewal charges. These regulatory fees form part of PAGCOR's oversight mechanism and support its mandate to ensure the integrity, fairness, and security of online gaming operations.

Audit fee

In addition to the applicable GGR Sharing, the Operator is required to pay an audit fee equivalent to ten percent (10%) of the PAGCOR Share. The audit fee is imposed in connection with the independent or third-party verification and audit of the operator's gaming transactions and reported Gross Gaming Revenue through PAGCOR's designated audit and monitoring systems. Accordingly, the audit fee is computed on the amount of the PAGCOR Share due, rather than directly on the operator's Gross Gaming Revenue, and is billed and remitted in accordance with PAGCOR's prescribed procedures.

Foundation fee

A Gaming System Administrator is further required to establish and maintain a foundation in accordance with PAGCOR's Implementing Rules and Guidelines for the Foundations of Gaming System Administrators. The principal source of funding of the foundation is a monthly contribution equivalent to one percent (1%) of the Gross Gaming Revenue generated from electronic games offered through the Gaming System Administrator's electronic gaming platform. The contribution must be remitted to a dedicated bank account maintained for the foundation and may be utilized only for projects and purposes permitted under PAGCOR's applicable rules and subject to the prescribed approval, monitoring, reporting, and audit requirements.

Monitoring Fees

Separately from PAGCOR's regulatory fees, online gaming operators remain subject to the national tax regime applicable to domestic corporations, including corporate income tax, value-added tax or percentage tax (as applicable), and withholding taxes on compensation and supplier payments. These taxes are payable to the Bureau of Internal Revenue and operate independently of PAGCOR's revenue-sharing framework.

Franchise tax

In addition, as a licensed operator in the Philippines, the Group is required to pay franchise tax on revenues generated from its gaming operations domestically to the Bureau of Internal Revenue in the Philippines, in lieu of all taxes, including value-added tax (VAT).

By order of the Board
International Entertainment Corporation
Ho Wong Meng
Chairman and Executive Director

Hong Kong, 28 August 2026

As at the date of this announcement, the Board comprises two executive Directors, namely Mr. Ho Wong Meng and Mr. Aurelio Jr. Dizon Tablante, and three independent non-executive Directors, namely Mr. Luk Ching Kwan Corio, Ms. Danica Ramos Lumawig and Mr. Brian Roger Mattingley.