Financial Services Regulatory Commission
Antigua and Barbuda
Division of Gaming

Customer Due Diligence Guidelines for

Interactive Gaming & Interactive Wagering Companies

November 2005

Customer Due Diligence for Interactive Gaming & Interactive Wagering Companies

I. Introduction

1. The risk of money laundering and terrorist financing is increasingly threatening to destroy the integrity of the financial system the world over. All the financial institutions, including those operating under the IBC Act, and the Interactive Gaming & Wagering Regulations are required to scrupulously comply with the requirement of the Money Laundering (Prevention) Act 1996, the Prevention of Terrorism Act, 2001 as well as the regulations and guidelines issued there under by the Office of Money Laundering and Drug Control Policy (ONDCP), which is the administering authority for the two legislations.

2. Over the last few years a number of international standards and best practices have been issued by the international bodies like the Basel Committee on Banking Supervision and Financial Action Task Force. In our view it is necessary for the jurisdiction to incorporate these standards and best practices in order to further enhance the clean image and integrity of the jurisdiction and to mitigate the risk the financial institutions operating in the jurisdiction may face due to possible exposure to the risk of money laundering and terrorist financing. Section 316 (4) of the IBC Act requires the FSRC to take any necessary action that is required to ensure the integrity of the international business corporation sector. Accordingly, these guidelines are being issued for gaming companies licensed to operate under the Interactive Gaming & Interactive Wagering Regulations, 2001, for compliance with immediate effect. Gaming companies are requested to take necessary action and report compliance by January 31, 2006. It is clarified that these instructions are meant to supplement and not supplant the provisions of the Money Laundering (Prevention) Act 1996 or the Prevention of Terrorism Act, 2001 or the regulations and guidelines issued by the ONDCP, which remains the primary agency for the administration of these laws. Therefore, in case of any conflict between the guidelines issued herein and the guidelines issued by the ONDCP, the higher requirement should be observed.

II. Importance of KYC standards for supervisors and Interactive Gaming and Interactive Wagering Corporations (IGIWC)

3. Adequate due diligence on new and existing customers is a key part of the internal controls in IGIWC to ensure that they do not become subject to reputational, operational, legal and concentration risks, as these can result in significant financial cost.

4. Sound KYC procedures have particular relevance to the safety and soundness of IGIWC, in that they:

- help to protect IGIWC reputation and the integrity of interactive gaming systems by reducing the likelihood of IGIWC becoming a vehicle for or a victim of financial crime and suffering consequential reputational damage;
- constitute an essential part of sound risk management (e.g. by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities, including assets under management).

5. The inadequacy or absence of KYC standards can subject IGIWC to serious customer and counterparty risks, especially **reputational, operational, legal and concentration risks**. All these risks are interrelated. However, any one of them can result in significant financial cost to IGIWC (e.g. through the withdrawal of funds by creditors, the termination of payment processors facilities, claims against the IGIWC, investigation costs, asset seizures and freezes, and receivable losses), as well as the need to divert considerable management time and energy to resolving problems that arise.

Reputational risk

6. It is defined as the potential that adverse publicity regarding an IGIWC business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the company. It poses a major threat to IGIWC since the nature of their business requires maintaining the confidence of creditors and the general marketplace. IGIWC are especially vulnerable to this risk because they can easily become a vehicle for or a victim of illegal activities perpetrated by their customers. They need to protect themselves by means of continuous vigilance through an effective KYC programme.

Operational risk

7. It can be defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. Most operational risk in the KYC context relates to weaknesses in the implementation of IGIWC programmes, ineffective control procedures and failure to practice due diligence. A public perception that on-line gaming is not able to manage its operational risk effectively which can disrupt or adversely affect the business of the company.

Legal risk

8. It is the possibility that lawsuits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of a IGIWC. On-line Gaming Companies may become subject to lawsuits resulting from the failure to observe mandatory KYC standards or from the failure to practice due diligence. Consequently, IGIWC can, for example, suffer fines, criminal liabilities and special penalties imposed by the regulatory authority. Indeed, a court case involving a gaming company may have far greater cost implications for its business than just the legal costs. IGIWC will be unable to protect themselves effectively from such legal risks if they do not engage in due diligence in identifying their customers and understanding their customer profile.

Concentration risk

9. The concentration risk applies both to the assets and liabilities side of the balance sheet. Without knowing precisely who the customers are, and their relationship with other customers, it will not be possible for a gaming company to measure its concentration risk.

10. On the liabilities side, concentration risk is closely associated with funding risk, particularly the risk of early and sudden withdrawal of funds by large depositors, with potentially damaging consequences for IGIWC liquidity. Funding risk is more likely to be higher in the case of small IGIWC. Analyzing deposit concentrations requires on-line gaming companies to understand the characteristics of their customers, including not only their identities but also the extent to which their actions may be linked with those of other customers. It is essential that liabilities managers in gaming companies not only know but maintain a close relationship with large depositors, or they will run the risk of losing their funds at critical times.

III. Essential elements of KYC standards

12. All IGIWC should have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the on-line gaming company from being used, intentionally or unintentionally, by criminal elements. KYC should be a core feature of IWIGC risk management and control procedures, and be complemented by regular compliance reviews and internal audit.

13. Certain key elements should be included by on-line gaming companies in the design of KYC programmes. Such essential elements should start from the company's risk management and control procedures and should include:

(1) customer acceptance policy,
(2) customer identification,
(3) on-going monitoring of high risk accounts and
(4) risk management.

IGIWC should not only establish the identity of their customers, but should also monitor account activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account. The intensity of KYC programmes beyond these essential elements should be tailored to the degree of risk.

1. Customer acceptance policy

14. IGIWC should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to a company. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, or other risk indicators should be considered.

Graduated Customer acceptance policy

15. IGIWC should develop graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers. For example, extensive due diligence would be essential for an individual with a high net worth whose source of funds is unclear. Decisions to enter into business relationships with higher risk customers, should be taken exclusively at senior management level.

2. Customer identification

17. Customer identification is an essential element of KYC standards. A customer includes:

- the person that is registered as the player to maintain an account with the on-line gaming company

18. IGIWC should establish a systematic procedure for identifying new customers and should not establish a relationship until the identity of a new customer is satisfactorily verified.

19. Gaming companies should document and enforce policies for identification of customers and those acting on their behalf. The best documents for verifying the identity of customers are those most difficult to obtain illicitly and to counterfeit. In no case should a company short-circuit identity procedures just because the new customer is unable to present required documentation.

20. The customer identification process applies at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a need for IGIWC to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change and/or unusual activity in the

way that the account is operated. However, if a company becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

General identification requirements

23. IGIWC need to obtain all information necessary to establish to their full satisfaction the identity of each new customer

24. When an account has been opened, but problems of verification arise in the customer relationship which cannot be resolved, the on-line gaming company should close the account and return the monies to the source from which they were received.

Enhanced due diligence for transferred accounts

25. While the transfer of an opening balance from another on-line gaming account in the customer's name to another on-line gaming company subject to the same KYC standard may provide some comfort, IGIWC should nevertheless consider the possibility that the previous account manager may have asked for the account to be removed because of a concern about dubious activities. If a on-line gaming company has any reason to believe that an applicant is being refused gaming facilities by another IGIWC, it should apply enhanced diligence procedures to the customer.

26. IGIWC should never agree to open an account or conduct ongoing business with a customer who insists on anonymity or who gives a fictitious name. Introduced business

30. Relying on due diligence conducted by an introducer, however reputable, does not in any way remove the ultimate responsibility of the IGIWC to know its customers and their business. In particular, IGIWC should not rely on introducers that are subject to weaker standards than those governing the company's own KYC procedures or that is unwilling to share copies of due diligence documentation.

31. The on-line gaming companies that use introducers should carefully assess whether the introducers are "fit and proper" and are exercising the necessary due diligence in accordance with the standards set out herein. The ultimate responsibility for knowing customers always lies with the company. IGIWC should use the following criteria to determine whether an introducer can be relied upon:

- it must comply with the minimum customer due diligence practices identified herein;
- the customer due diligence procedures of the introducer should be as rigorous as those which the gaming company would have conducted itself for the customer;
- the on-line gaming company must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer;

- the on-line gaming company must reach agreement with the introducer that it will be permitted to verify the due diligence undertaken by the introducer at any stage; and
- all relevant identification data and other documentation pertaining to the customer's identity should be immediately submitted by the introducer to the on-line gaming company, who must carefully review the documentation provided. Such information must be available for review by the Commission, ONDCP or any other competent authority.

In addition, IGIWC should conduct periodic reviews to ensure that an introducer continues to conform to the criteria set out above.

Non-face-to-face customers

39. A typical example of a non-face-to-face customer is one who wishes to conduct gaming via the Internet or similar technology. As a basic policy IGIWC should proactively assess various risks posed by emerging technologies and design customer identification procedures with due regard to such risks.

40. In accepting business from non-face-to-face customers IGIWC should take specific and adequate measures to mitigate the higher risk. Examples of measures to mitigate risk include: certification of documents presented; requisition of additional documents to complement those which are required for face-to-face customers; independent contact with the customer by the bank (*ISSUING BANK OF CREDIT CARD);* third party introduction, e.g. by an introducer subject to the criteria mentioned in paragraph 31; or requiring the first payment to be carried out through an account in the customer's name with another bank subject to similar customer due diligence standards.

Alternative Payment Processing

41. Alternative Payment Processing is the provision of on-line payment services by an e-payment company to an IGIWC. If IGIWC fail to apply due diligence to their merchant accounts, they expose themselves to the range of risks identified earlier, and may find themselves holding and/or transmitting money linked to corruption, fraud or other illegal activity.

42. IGIWC should gather sufficient information about their alternative payment providers to understand fully the nature of their business. Factors to consider include: information about the company's management, major business activities, where they are located and its money-laundering prevention and detection efforts; and the condition of the regulation and supervision in the company's country.

43. IGIWC should only establish merchant relationships with e-payment providers that are effectively supervised by the relevant authorities. For their part, e-payment providers should have effective customer acceptance and KYC policies.

3. On-going monitoring of accounts and transactions

46. On-going monitoring is an essential aspect of effective KYC procedures. IGIWC can only effectively control and reduce their risk if they have an understanding of normal and reasonable account activity of their customers so that they have a means of identifying transactions which fall outside the regular pattern of an account's activity. Without such knowledge, they are likely to fail in their duty to report suspicious transactions to the appropriate authorities in cases where they are required to do so.

47. The extent of the monitoring needs to be risk-sensitive. For all accounts, IGIWC should have systems in place to detect unusual or suspicious patterns of activity. This can be done by establishing limits for a particular class or category of accounts. Particular attention should be paid to transactions that exceed these limits. Certain types of transactions should alert IGIWC to the possibility that the customer is conducting unusual or suspicious activities. They may include transactions that do not appear to make economic sense, or that involve large amounts of deposits that are not consistent with the normal and expected transactions of the customer. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account. Examples of suspicious activities can be found in the Guidelines issued by the ONDCP.

Higher risk accounts

48. There should be intensified monitoring for higher risk accounts. Every IGIWC should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin and source of funds, the type of transactions involved, and other risk factors.

49. For higher risk accounts IGIWC should ensure that they have adequate management information systems to identify, analyze and effectively monitor higher risk customer accounts. Senior management should know the personal circumstances of the company's high risk customers and be alert to sources of third party information. Significant transactions by these customers should be approved by a senior manager. IGIWC should develop clear policy and internal guidelines, procedures and controls and remain especially vigilant regarding as it relates to such accounts.

4. Risk management

Policies and procedures

50. The board of directors and compliance officers of the IGIWC should be fully committed to an effective KYC programme by establishing appropriate procedures and ensuring their effectiveness. Explicit responsibility should be allocated within the IGIWC for ensuring that the company's policies and procedures are managed effectively and are, at a minimum, in accordance with the laws and regulations of Antigua and Barbuda.

The channels for reporting suspicious transactions should be clearly specified in writing, and communicated to all personnel.

Internal audit and compliance

51. IGIWC internal audit and compliance functions have important responsibilities in evaluating and ensuring adherence to KYC policies and procedures. As a general rule, the compliance function should provide an independent evaluation of the company's own policies and procedures, including legal and regulatory requirements. Its responsibilities should include ongoing monitoring of staff performance through sample testing of compliance and review of exception reports to alert senior management or the Board of Directors if it believes management is failing to address KYC procedures in a responsible manner.

52. Internal audit plays an important role in independently evaluating the risk management and controls, discharging its responsibility to the Audit Committee of the Board of Directors or a similar oversight body through periodic evaluations of the effectiveness of compliance with KYC policies and procedures, including related staff training. Management should ensure that audit functions are staffed adequately with individuals who are well versed in such policies and procedures. In addition, internal auditors should be proactive in following-up their findings and criticisms.

Know your employees

53. The integrity of a financial institution is heavily dependent on the integrity of its employees, as it is the employees who are responsible for implementing its policies and programmes. The licensed institutions should put in place adequate screening procedures to ensure high standards when hiring employees.

Employees training

54. All IGIWC must have an ongoing employee-training programme so that company's staff is adequately trained in KYC procedures. Training requirements should have a different focus for new staff, front-line staff, compliance staff or staff dealing with new customers. New staff should be educated in the importance of KYC policies and the basic requirements at the company. Front-line staff members who deal directly with the customer should be trained to verify the identity of new customers, to exercise due diligence in handling accounts of existing customers on an ongoing basis and to detect patterns of suspicious activity. Regular refresher training should be provided to ensure that staff are reminded of their responsibilities and are kept informed of new developments. It is crucial that all relevant staff fully understand the need for and implement KYC policies consistently. A culture within the company that promotes such understanding is the key to successful implementation.

IV. Implementation of KYC standards in a cross-border context

55. All Parent IGIWC licensed in Antigua and Barbuda must communicate their KYC policies and procedures (which must meet the standards set herein) to their overseas offices and subsidiaries, and have a routine for testing compliance against both Antigua and Barbuda and host country KYC standards. Such compliance tests should also be tested by internal and external auditors.

56. A senior officer should be designated to be directly responsible for ensuring that all relevant staff are trained in, and observe, KYC procedures that meet both home and host standards. While this officer will bear primary responsibility, he should be supported by internal auditors and compliance officers from both local and head offices as appropriate.

57. Where the minimum KYC standards of the host countries differ from those of Antigua and Barbuda, offices, subsidiaries in the host jurisdictions should apply the higher standard of the two. If, however, local laws and regulations (especially secrecy provisions) prohibit the implementation of Antigua and Barbuda's KYC standards, where the latter are more stringent, overseas offices and subsidiaries would have to comply with host country standards, but they should make sure to inform their head office or parent IGIWC which in turn must inform the Director of Gaming about the nature of the difference.

58. IGIWC should be aware of the high reputational risk of conducting business in jurisdictions that have lower or inadequate KYC standards. Parent companies should have a procedure for reviewing the vulnerability of the individual operating units and implement additional safeguards where appropriate. If necessary, the Commission and/or the ONDCP should be consulted.

V. Terrorist Financing

59. The risk of IGIWC being used as conduits for transfer of funds involved in terrorist financing has increased significantly in recent years. IGIWC deemed as financial institutions are prohibited from carrying out any transactions with terrorists or terrorist organizations under the Prevention of Terrorism Act, 2001. All IGIWC must comply with any guidelines issued by the ONDCP in this regard. If a company suspects or has reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organisations, it should report promptly their suspicions to the competent authorities.

Credit Card & Debit Cards

65. When credit or debit cards are used as a payment system to affect a money transfer, they are covered by these guidelines, and the necessary information should be included in the message.