ML/TF NATIONAL RISK ASSESSMENT
RESULTS AND IMPLICATIONS FOR THE GAMING SECTOR

10TH OCTOBER 2018
Introductions

DR. DOMINIK MICALLEF
Chief Officer Enforcement
Malta Gaming Authority
## Agenda

<table>
<thead>
<tr>
<th>Topic</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. National Risk Assessment: Sector-Specific Findings</strong></td>
<td>12:00</td>
</tr>
<tr>
<td>Context</td>
<td></td>
</tr>
<tr>
<td>Gaming outcomes</td>
<td></td>
</tr>
<tr>
<td><strong>2. Implications for private sector</strong></td>
<td>12:20</td>
</tr>
<tr>
<td>AML/CFT controls framework</td>
<td></td>
</tr>
<tr>
<td>Guidance to private sector</td>
<td></td>
</tr>
<tr>
<td>Reference sources for further guidance</td>
<td></td>
</tr>
<tr>
<td><strong>3. Questions</strong></td>
<td>12:45</td>
</tr>
<tr>
<td><strong>4. Concluding Remarks</strong></td>
<td>12:55</td>
</tr>
</tbody>
</table>
Part 1 National Risk Assessment: Sector-Specific Findings
Context
This session builds on the seminar hosted yesterday, focusing on the specific implications of the results of the National Risk Assessment

Yesterday

• Provided a general overview of Malta’s ML / TF National Risk Assessment
  – Introduced context and methodology
  – Presented high-level results

• Presented response of competent authorities
  – Communicated National AML/CTF Strategy
  – Highlighted importance of private sector contribution to the national effort

Today

• Specific focus on ML / TF risks facing the Gaming sector
  – Sets out methodology for sector-specific risk assessments
  – Presents results of NRA from perspective of the gaming sector

• Outlines implications of findings and how the private sector can effectively respond
  – Establishes role of private sector in mitigating ML / TF risks
  – Advises on best practice for client due diligence / risk assessment processes
Context
This session aims to ensure the Gaming sector understands the ML/FT risks facing them, and how they can help to mitigate these risks

Be aware of money laundering/terrorist financing risks and results of the National Risk Assessment

Be prepared to communicate these risks and their implications both internally and externally

Understand what actions can be taken at an institutional level to combat these risks
Gaming outcomes
Inherent vulnerabilities in the gaming sector stem from four key sources

- Customer Risk
- Product/Service/transaction risk
- Interface Risk
- Geographical Risk
### Inherent risk – Funding Methods

<table>
<thead>
<tr>
<th>Payment Method</th>
<th>Low</th>
<th>Low-Medium</th>
<th>Medium</th>
<th>Medium-High</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank transfers (EEA or equivalent safeguards)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Debit/credit cards issued by banks (EEA or equivalent safeguards)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Debit/credit cards issued by other licensed financial institutions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EEA-licensed payment service providers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-EEA licensed PSP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EEA-Licensed PSP that can be funded with cash or quasi-cash</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prepaid cards/vouchers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Gaming outcomes
Deep-dive on inherent risk and controls effectiveness

## Inherent risk – Game Types

<table>
<thead>
<tr>
<th></th>
<th>Low-Medium</th>
<th>Medium</th>
<th>Medium-High</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed odds games without hedging (ex: slots, lotteries, bingo)</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fixed odds games where hedging is possible (blackjack, baccarat, roulette)</td>
<td></td>
<td>High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sports betting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P2P games (ex: Poker, betting exchange)</td>
<td></td>
<td></td>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>
Gaming outcomes
Deep-dive on inherent risk and controls effectiveness

Inherent risk – Channels

<table>
<thead>
<tr>
<th>Channel</th>
<th>Low-Medium</th>
<th>Medium</th>
<th>Medium-High</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote &amp; automated registration on an electronic platform without 3rd party intervention</td>
<td>Green</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facilitation of registration by a land-based intermediary</td>
<td></td>
<td></td>
<td>Pink</td>
<td></td>
</tr>
<tr>
<td>Use of master account set-up</td>
<td></td>
<td></td>
<td></td>
<td>Red</td>
</tr>
</tbody>
</table>
Part 2  Implications for private sector
AML/CFT controls framework
To effectively manage ML/TF risk, institutions must develop effective AML/CFT capabilities across the board

Public controls

- Market entry restrictions
  - Regulatory barriers to entry designed to ensure companies and institutions are established for genuine purposes
  - Includes registration of all entities, in addition to licensing of specific higher-risk sectors

- Ongoing oversight and monitoring
  - Monitoring and regulation of ongoing business activities by competent authorities
  - Includes passive reporting and active supervisory action (e.g. on-site visits)

- Detection, investigation and prosecution
  - Detection of ML/TF activity and subsequent action taken
  - Includes various detection mechanisms (e.g. suspicious transaction reporting), as well as investigatory, judicial and sanction/recovery processes

Private controls

- Individual institutions’ AML/CFT frameworks
  - Controls established within individual institutions to prevent and detect ML/TF through that organisation
  - Include various control elements across the AML/CFT life-cycle, from due-diligence during customer acquisition process to procedures in place to detect and report suspicious activity
  - Follows a risk-based approach, with control severity proportional to the riskiness of the client/product in question

Focus of this session
AML/CFT controls framework
Gaming entities should have perform an AML/CFT risk assessment across the various types of risk and develop a customer acceptance policy

Conducting the AML/CFT Risk Assessment

Perform AML/CFT – Business Risk Assessment

Produce Customer Acceptance Policy

High risk customer
Medium risk customer
Low risk customer
### Guidance on strengthening controls

Examples of mitigating measures across Funding Methods

#### Funding Methods

1. **Jurisdiction of Operation, and the regulatory environment relating to payments**
2. **Methods used in processing payment of winnings to players (including procedures used when payments cannot be performed to the account of origin)**
3. **Methods used in identifying origin of payments (ex: confirming that the account holder with the bank, card-issuer, or payments institution is the same as the gaming account holder)**
4. **Strength of the Operator’s payments and anti-fraud team**
5. **Effectiveness of the operator’s technological tools in place to monitor and detect suspicious activity**
Guidance on strengthening controls
Examples of mitigating measures across Game Types

Game Types

1. Strength of Operator’s anti-fraud and anti-collusion department
2. Other safeguards against collusion
   (e.g., impossibility of a player choosing his or her opponent)
3. Effectiveness of the operator’s technological tools in place to monitor, prevent and detect fraud or collusion
   (e.g., automated alerts on suspicious gameplay, chatroom/forum monitoring dynamic and responsive risk management processes)
4. Level of monitoring for sports integrity
Guidance on strengthening controls
Examples of mitigating measures across Channels

Channels

1. Effectiveness of onboarding procedures and associated safeguards
2. Effective control over land-based intermediary and access controls
3. Techniques used for monitoring of player activity
4. Regulatory environment and effective supervision carried out by local authorities
Reference sources for further guidance

• SUBSIDIARY LEGISLATION 373.01 PREVENTION OF MONEY LAUNDERING AND FUNDING OF TERRORISM REGULATIONS -

• FIAU | MGA Implementing Procedures for the Remote Gaming Sector -

• FIAU | MGA Implementing Procedures for Land Based Casinos

• Implementing Procedures Part 1 (as of January 2017, to be updated) -

• Section 2 of the FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing - High Level Principles and Procedures.

• Additional insights into the risk-based approach can be derived from the FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing - High Level Principles and Procedures.

• The European Commission - Supranational Risk Assessment Report on the 26th June 2017.

• FATF High-risk and other monitored jurisdictions - http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)
Q&A
Part 4 | Concluding remarks
Looking ahead

What you can do

• Assess your business risks in terms of AML/CFT
  – Geographical Risk
  – Customer Risk
  – Interface Risk
  – Product Risk
• Act on a risk based approach
• Identify, Verify and Monitor
• Obtain additional information when necessary; (e.g. additional verification documentation, source of wealth/funds)
• Apply thorough record keeping
• When a subject person detects a suspicious transaction related to AML/CFT, shall escalate a Suspicious Transaction Report (STR)
• Avoid disclosures at all times

What we will do

• Examine subject persons in light of new obligations and provide the necessary guidance
• Outreach sessions in light of new ML/TF typologies
• Provide sector specific guidance in terms of AML/CFT via official publications and updating implementing procedures
• Share lessons learned and new mitigation control methods
Appendix  |  Additional information
Customer risk: The risk of ML/FT may vary in accordance with the type of customer. The assessment of the risk posed by a natural person is general based on the person’s economic activity and/or source of wealth. A Customer having a single source of regular income will pose a lesser risk of ML/FT than a customer who has multiple sources of income or irregular income streams.
**Product/Service/Transaction Risks**: Some products/services/transactions are inherently riskier than others and are therefore more attractive to criminals. These include products/services/transactions which are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the customer to influence the outcome of a game, be it on his own or in collusion with others.

The use by customers and the acceptance by licensees of specific funding methods should also be treated as high risk factors. This includes *cash* and other similar or *anonymous payment methods* that may not leave or disrupt the audit trail, and allow the customer to operator with a degree of or complete anonymity such as *pre-aid cards or virtual currencies*.

The exceptional use by a customer of accounts held or cards issued in the name of third parties is also to be regarded as a high risk factor. Conversely where a customer transfers funds from a bank account or a card linked to a bank account held in his name with an institution established in a reputable jurisdiction, the risk of ML decreases – these credit or financial institutions established in a reputable jurisdiction, the risk of ML decreases – these credit or financial institutions are themselves subject persons and one would expect that as part of their CDD obligations they would monitor on an on-going basis any account or card activity.
Interface Risks: The channels through which a licensee establishes a business relationship and/or through which transactions are carried out may also have a bearing on the risk profile of a business relationship or a transaction. **Channels that favour anonymity increase the risk of ML/TF if no measures are taken to address the same**

While situations where interaction with the customer takes place on a non-face to face basis will no longer lead to the relationship being considered as automatically high risk, interacting in this manner is still to be considered as high risk factor for risk assessment purposes unless the licensee adopts technological measures and controls to address the heightened risk of identity fraud or impersonation present in these situations.
Geographical Risk: The geographical risk is the risk posed to the licensee by the geographical location of the business/economic activity and the source of wealth/funds of the business relationship. The nationality, residence and place of birth of a customer have to be taken into account as these might be indicate of a heightened geographical risk.

Countries that have a weak AML/CFT system, countries known to suffer from a significant level of corruption countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction as well as countries which are known to have terrorist organisation operating within are to be considered as high risk. The opposite is also true and may therefore be considered as presenting a medium or low risk of ML/TF.
Laundering via gambling sites
A perpetrator uses gambling sites to deposit illicit funds and to request the pay out of winnings or unplayed balance. Legitimate online gambling accounts are credited with dirty funds (deposit) followed by gambling on only small amount of funds (including very low volatility games) or transferring the remaining funds to a different player, or to a different online gambling operator. The remaining funds are cashed out as if they were legitimate gambling earnings.

Smurfing
Criminals may use several "smurfs" betting directly against each other using dirty funds. One of the "smurfs" will receive all the funds as an apparent winner, who will then cash out the funds as if they were legitimate gambling earnings.
Risk Scenarios to be aware of (2/2)

Purchase of online casino accounts
Criminals may purchase online casino accounts containing funds already uploaded by non-criminal players at a higher price than the real one. They may also invent and bet on fictitious (non-existing) matches or events to ensure winnings.

Purchasing of winning tickets
Purchasing of winning tickets especially where betting is involved.
Guidance on strengthening controls (1/3)

AML/CFT Control Mechanisms

Start

New customer registers

Apply minimum CDD level

Ongoing monitoring

Customer reaches €2,000 deposit threshold within 180 days

PEP Check

Name and surname/permanent residential address/date of birth
Guidance on strengthening controls (2/3)

Classify customer risk
- Low risk customer
  - Verification of personal details
  - Ongoing monitoring to ensure relationship remains low risk and threshold not exceeded
  - Report suspected cases of ML/TF
- Medium risk customer
  - Collect additional personal details
  - Verify using documents with photograph
  - Collect source of wealth information if no statistical models are used
  - On-going monitoring to detect unusual activities, and keep information and profile updated
  - Report suspected cases of ML/TF
- High risk customer
  - Collect additional personal details
  - Verify using documents with photograph
  - Collect source of wealth information and documentation
  - Enhance on-going monitoring to detect unusual activities, and keep information and profile updated
  - Take additional measures to address any other risks identified
  - Report Suspected Cases of ML/TF

Is customer a PEP?
- Yes
  - Obtain senior management approval to service PEP
  - Establish what is their source of wealth and where applicable, their source of funds
  - Conduct enhanced on-going monitoring of the customers activity
- No
  - Place of birth/nationality/identify reference number
  - Verify documentation
  - Low risk customer
  - Medium risk customer
  - High risk customer
Guidance on strengthening controls (3/3)

Did customer provide verification and additional documentation (as necessary) within 30 days?

- Yes
  - Perform on-going monitoring to detect unusual activities and keep information and profile up to date
  - End

- No
  - Terminate the business relationship and, once ascertained that there are no restriction on the transfer or release of the funds, transfer the funds back to the original source using the same channels through which received
  - Consider whether there are grounds to file a Suspicious Transaction Report with FIAU