ANTI-MONEY LAUNDERING AND ONLINE GAMBLING

GUIDANCE ON HOW TO IMPLEMENT BROAD AND INDISTINCT AML NOTIONS IN REGULATORY PRACTICE
Anti-Money Laundering and Online Gambling

Guidance on How to Implement Broad and Indistinct AML Notions in Regulatory Practice

Dr Simon Planzer, M.A., Esq.
Lecturer in Law

University of St.Gallen
# Table of Contents

List of Figures ..............................................................................................................................5
List of Acronyms ..........................................................................................................................6

1. Introduction ............................................................................................................................7
   1.1. The Research Question .....................................................................................................7
   1.2. Background and Relevance of Research .........................................................................8
      1.2.1 The AMLD and Gambling ..........................................................................................8
      1.2.2 Relevance of the Research beyond Gambling and the EU .........................................8
   1.3. Methodology ....................................................................................................................9
   1.4. Limitations .....................................................................................................................12

2. Money Laundering – An Introduction ..................................................................................13
   2.1. What is Money Laundering? ............................................................................................13
   2.2. Money Laundering and the AMLD ................................................................................13
   2.3. The Money Laundering Cycle ..........................................................................................14
      2.3.1 Placement Stage .........................................................................................................15
      2.3.2 Layering Stage ............................................................................................................16
      2.3.3 Integration Stage ........................................................................................................17

3. Interpretative Guidance .........................................................................................................20
   3.1 “The Business Relationship Is Conducted in Unusual Circumstances” .........................20
      3.1.1 General Remarks .......................................................................................................20
      3.1.2 Gambling Regulators ...............................................................................................20
      3.1.3 Who Should Define “Unusual”? ................................................................................21
         3.1.3.1 The Legislator? ..................................................................................................21
         3.1.3.2 Nullum Crimen et Nulla Poena Sine Lege ..............................................................22
      3.1.3.3 Who Is Able to Define “Unusual”: Regulator or Obliged Entity? .........................23
      3.1.4 How Can Obliged Entities Detect the “Unusual”? .......................................................23
      3.1.5 Customer Profile .......................................................................................................24
         3.1.5.1 KYC: Yes. But also “KYB”!.................................................................................24
         3.1.5.2 Profile Contents .................................................................................................25
      3.1.6 Monitoring .................................................................................................................26
      3.1.7 Unusual Higher Risk Behaviour: Experiences from the Financial Sector ................27
      3.1.8 Higher Risk: Are There Abstract Early Indicators? ....................................................29
      3.1.9 Higher Risks Through Transactional Circumstances ................................................31
   3.2 “Legal Persons or Arrangements that Are Personal Asset-Holding Vehicles” ..................33
3.6.2 Are New Products Automatically Higher Risk? .......................................................... 55
3.7 "Financial Products or Services that Provide Appropriately Defined and Limited Services to Certain Types of Customers, so as to Increase Access for Financial Inclusion Purposes" .......... 57
   3.7.1 Online Gambling Regulators .................................................................................. 57
   3.7.2 Defining Lower Risk? ............................................................................................. 57
   3.7.3 What Is Financial Inclusion? .................................................................................... 58
   3.7.4 Relevance for Online Gambling Sector? ................................................................. 58
   3.7.5 The Example of Hawala .......................................................................................... 58
3.8 "Products where the Risks of Money Laundering and Terrorist Financing are Managed by other Factors such as Purse Limits or Transparency of Ownership (e.g. Certain Types of Electronic Money)" ................................................................. 61
   3.8.1 Online Gambling Regulators .................................................................................. 61
   3.8.2 Prepaid Cards and E-Wallets ................................................................................. 61
   3.8.3 Transparency of Ownership ................................................................................... 61
4. Mitigating the Risks ........................................................................................................ 63
5. Conclusion ....................................................................................................................... 67
6. Acknowledgments ........................................................................................................... 70
Bibliography ..................................................................................................................... 72
List of Figures

Figure 1: The Money Laundering Cycle .................................................................................................................. 15
Figure 2: Money Laundering in Practice ................................................................................................................. 18
Figure 3: Hawala ....................................................................................................................................................... 59
### List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMLD</td>
<td>Fourth EU Anti-Money Laundering Directive</td>
</tr>
<tr>
<td>AML</td>
<td>Anti-Money Laundering</td>
</tr>
<tr>
<td>ATM</td>
<td>Automated Teller Machine</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Diligence</td>
</tr>
<tr>
<td>CFT</td>
<td>Combating the Financing of Terrorism</td>
</tr>
<tr>
<td>EEA</td>
<td>European Economic Area</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>FCA</td>
<td>(United Kingdom) Financial Conduct Authority</td>
</tr>
<tr>
<td>FinCEN</td>
<td>Financial Crimes Enforcement Network</td>
</tr>
<tr>
<td>FINMA</td>
<td>Swiss Financial Market Supervisory Authority</td>
</tr>
<tr>
<td>FinTech</td>
<td>Financial Technology</td>
</tr>
<tr>
<td>FIU</td>
<td>Financial Intelligence Unit</td>
</tr>
<tr>
<td>FMA</td>
<td>Financial Market Authority of Liechtenstein</td>
</tr>
<tr>
<td>GREF</td>
<td>Gaming Regulators European Forum</td>
</tr>
<tr>
<td>IMF</td>
<td>International Monetary Fund</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>MONEYVAL</td>
<td>Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism</td>
</tr>
<tr>
<td>MROS</td>
<td>Money Laundering Reporting Office of Switzerland</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation of Economic Co-operation and Development</td>
</tr>
<tr>
<td>PEP</td>
<td>Politically Exposed Person</td>
</tr>
<tr>
<td>PI</td>
<td>Primary Investigator</td>
</tr>
<tr>
<td>RBA</td>
<td>Risk-Based Approach</td>
</tr>
<tr>
<td>SAR</td>
<td>Suspicious Activity Report</td>
</tr>
<tr>
<td>STR</td>
<td>Suspicious Transaction Report</td>
</tr>
<tr>
<td>TEU</td>
<td>Treaty on the European Union</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
</tbody>
</table>
1. Introduction

1.1. The Research Question

Gambling regulators are currently facing the challenge of implementing the requirements of the Fourth EU Anti-Money Laundering Directive (AMLD). The directive refers to circumstances of “lower” money laundering risks as well as “higher” money laundering risks. In the latter case, obliged entities shall apply enhanced customer due diligence.

However, the notions describing these circumstances are often broad and indistinct. For instance, the AMLD foresees enhanced customer due diligence when “the business relationship is conducted in unusual circumstances”. Confronted with these notions, gambling regulators are facing the following challenge:

What do these broad and indistinct notions mean when applied to the gambling industry, more specifically, the online gambling industry?

Regulators may further wonder, how they can specify effective regulatory AML requirements without unnecessarily burdening their gambling industry.

As the AMLD applies to online gambling, too, there is significant uncertainty in the online gambling industry as to the AML standards that the industry is supposed to comply with. Regulated operators have a vital interest in fully complying with AML provisions at all levels (EU; national law; regulator): the sanctions for non-compliance can reach from high fines, over the freezing of customer accounts to the withdrawal of the operator’s license.

Through directives, the EU intends to harmonise the national rules of its 28 Member States in a certain area. Directives generally leave some discretion to Member States as per how to implement these rules in national law. Moreover, some directives give Members States the possibility to adopt or retain stricter provisions. This is also the case with the AMLD. Online gambling operators - often licensed in numerous EU jurisdictions - fear that they will be confronted with 28 different sets of

---

1 In the present report, the term „gambling“ is used to refer to games of chance. The AMLD too uses this term.
3 Article 18(3) AMLD.
4 Annex III AMLD.
6 EU membership base as per September 2017. At this point in time, the British exit from the EU had not yet taken legal effect.
7 Article 5 AMLD.
AML rules that significantly vary from one country to another. This would further increase the compliance burden on the online gambling industry. Recent years have seen major mergers among operators, often driven by the attempt to cut down costs, not least for compliance-related work. With the increase of the compliance burden, as with any costs, comes also a certain risk that financial resources for innovation will be cut.

In short, the research shall answer the following:

*How are the broad and indistinct notions referring to lower or higher money laundering risks to be interpreted? And how are they to be interpreted specifically in relation to online gambling services?*

### 1.2. Background and Relevance of Research

#### 1.2.1 The AMLD and Gambling

The European Parliament adopted the AMLD on May, 20th 2015. The European Union hereby aims to strengthen the existing anti-money laundering framework in order to “follow the money and crack down on money laundering and terrorist financing.” The AMLD is of direct relevance for gambling regulators in the EU and the EEA. However, the findings of this report are of relevance for regulators globally as will be outlined below.

As far as games of chance were concerned, the predecessor directive (3rd AML Directive) was only applicable to land-based casinos. By contrast, the scope of the AMLD encompasses the whole gambling industry. Importantly, it includes for the first time the online gambling industry, too: gambling services that are provided “by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of service.”

Some EU Member States have implemented the AMLD, others have not done so yet. In any event, early guidance to regulators by way of this report can be useful since regulators will have to develop an AML policy, possibly in conjunction with their colleagues from the national FIU.

#### 1.2.2 Relevance of the Research beyond Gambling and the EU

This report puts the focus on online gambling. Yet, its relevance goes beyond gambling. The AMLD has to be implemented in numerous industries. Accordingly, other regulatory authorities and professionals from other industry may find this report helpful, too. They too have to apply the same abstract AML notions. And they must give real life meaning to these notions – as does this report.

---

9 Article 2 para. 1. (3)(f) AMLD.
10 Article 3(14) AMLD.
11 AMLD, Article 67(1). The AMLD entered into force on June, 26th 2015, and all 28 Member States had until June, 26th 2017 to implement the AMLD into domestic law.
The geographic relevance of the report goes far beyond the EU. Authorities in most countries will have to apply abstract AML notions to real life constellations. In many cases, these notions will be strikingly similar to those presented in this report, for the following reason.

The AMLD is not an isolated initiative of the European Union. Apart from other international actors, the driving force behind the revised EU directive is the Financial Action Task Force (FATF). And many notions used in the AMLD find their origins in FATF work, for instance the FATF recommendations.

The FATF is an inter-governmental body established in 1989. It is composed of 35 countries plus the European Commission and the Gulf Cooperation Council. The FATF is a policy making body: it sets standards and promotes effective measures against money laundering and, notably after September 11, terrorist financing. It works to “generate the necessary political will to bring about national legislative regulatory reforms”. Apart from EU countries, its membership base includes: Argentina, Australia, Brazil, Canada, China, Hong Kong, Iceland, India, Japan, South Korea, Malaysia, Mexico, New Zealand, Norway, Russia, Singapore, South Africa, Switzerland, Turkey, United States; plus observer countries (e.g., Israel), observer organizations (e.g., Interpol), and associate members (e.g., Caribbean Financial Action Task Force).

It is further noteworthy that the FATF works through the secretariat of the Organisation for Economic Co-operation and Development (OECD) in Paris. In recent years, the OECD has set benchmarks against tax avoidance. And by way of naming and shaming non-compliant third countries it pressures those countries to adhere to OECD benchmarks. Accordingly, the AML standards that the FATF has defined in its recommendations are not only relevant for its members but are increasingly seen as a benchmark towards third countries, too.

The FATF has developed a series of official recommendations, published first in 1990. The most important revision dates from 2012 and the EU’s AMLD was significantly informed by these 40 recommendations.

1.3. Methodology

The objective of the research was to offer practical real life guidance to regulators. Broad and indistinct notions relating to lower or higher money laundering risks had to be fleshed out.

Different research methods were used to gather relevant information from professionals and the literature (desk research, feedbacks through questionnaire, interviews, literature review). The research consisted of several work packages.

---

13 FATF (no date) Co-operation Council for the Arab States of the Gulf (GCC).
14 FATF (no date) FATF members and observers.
• *Desk research, questionnaire and gambling regulators*

The work was initiated by desk research. The AMLD was closely analysed with a view of identifying all broad and indistinct circumstances that relate to lower or higher money laundering risks. Nine passages were identified and integrated in an online questionnaire (“SurveyMonkey”). The questionnaire was sent to five European gambling authorities of which three completed the online form.

In relation to each passage, the questionnaire asked what the authority’s provisional interpretation of the notion was; whether the authority had identified questions or difficulties in implementing the notion; and finally which sources / institutions / persons the authority would contact if it had to give conclusive meaning to the notion. The participants answered the questions comprehensively with very few exceptions.

The purpose of this work package was to gather online gambling-specific considerations and also challenges that regulators may face. In order to facilitate frank and open responses all participating authorities were assured that the report would not quote the specific regulator in relation to the provided input. The three participating gambling authorities provided valuable feedback, which is hardly surprising since they feature significant experience in regulating online gambling. Their experience was the key criterion for approaching them in the first place. The three authorities are recognised in this report in the acknowledgement section.

• *Expert interviews (AML professionals)*

Expert interviews in person or via phone call were arranged with representatives of institutions and other professionals that feature substantial expertise in the field of AML. It should be noted that the AMLD was not composed specifically for the online gambling sector but has general applicability. Accordingly, it seemed appropriate to acquire a holistic understanding of lower or higher risk circumstances. For that reason, the PI chose AML professionals for this work stream, most of whom have no particular relation to or experience in gambling matters.

A qualitative in-depth interview method was applied. The PI had a list of questions that included the nine passages. They were asked in the predefined order. But for the rest, the participants were granted sufficient discretion to express their views, provide concrete examples or freely elaborate on the topic more generally. This allowed in particular gathering valuable background information on the topic as well as on the rationale by which authorities have been driven in this field. The method also allowed deepening aspects that seemed particularly relevant for the research purpose.

Four representatives of authorities that were contacted did not respond or chose not to contribute. In discussions with another representative it became clear that his authority would not be able to contribute significantly. Eight persons fully contributed of which seven are recognised in the acknowledgement section.
• **Meetings with European Commission**

Officials working on AML matters at the European Commission were kind enough to invite the PI to meetings relating to the research topic. More precisely, the PI attended two meetings that looked at AML risks in the gambling sector. The PI further used these occasions for additional informal discussions with EU staff members, notably on aspects relevant for the research purpose. The officials are recognised in the acknowledgement section.

• **Literature review**

A literature review was performed in parallel to the aforementioned work packages. The PI initially intended that empirically driven works featuring empirical evidence in relation to AML issues would be given particular weight. However, the review showed that hardly any publication met this criterion.

The review was completed at the Central Library in Zurich and the European Commission Library in Brussels. The library catalogues were searched for books and other printed works; EBSCO and ProQuest were searched for electronic resources. In addition, relevant documents were searched on websites of organisations that are active in AML matters such as FATF, FinCEN, FINMA and MONEYVAL. Searches were done in English and German language.

A systematic research approach was applied from the outset to make the identification of the most relevant literature more likely. Search terms were amended depending on the number of initial hits. For instance, if a search created hundreds or thousands of hits, additional search terms were added that further targeted the search.

The websites of organisations active in AML work were initially searched with the terms “anti-money laundering”, “AML” and “Geldwäsche/Geldwäscherei”. Where the results were too numerous, the search was limited with the additional terms “risk factors” or “implementation”. Where the PI became aware of further relevant documents during the course of the research work, they were also added to the reading list.

In the Central Library the search terms “anti-money laundering” and “risk” were used as well as the equivalent terms in German language. For the databases EBSCO and ProQuest the search terms "anti-money laundering" and "risk factors" or “threat” or “vulnerability” were used.

Finally, the search in the European Commission Library was focused from the outset on relevance 3 works. The search was done with the terms “anti-money laundering” or “AML”. The search was refined by selecting “books” that were limited to the Library and e-Resource Centre Brussels. The same was performed with the terms “money laundering” or “AML”.

The bibliography in this report contains a long list of AML-related publications that stems from the aforementioned extensive literature search. A good part of it provided information on general AML
aspects; it can serve for future research, too. However, only a smaller part featured directly applicable relevance for the very specific research task at hand.\textsuperscript{16}

- \textit{Report}

All research elements informed the present report. In relation to each notion, the report first takes note of the responses provided by the gambling authorities. Subsequently, the report provides interpretative guidance in relation to each notion. The guidance is informed by the literature and the expert interviews; if possible, it is illustrated by practical examples. A general section explains how money laundering works in practice; it precedes the interpretative guidance in relation to the aforementioned notions.

1.4. Limitations

This research focused on AML issue relating to online gambling services. This was done for a number of reasons. In many jurisdictions gambling regulators have less experience in addressing online issues compared to land-based issues, including in the field of AML. Second, there are often fears among regulators (unfounded or founded) that online issues would be more complex than terrestrial issues. Third, focusing on online matters reduced the risk of overburdening the scope of the research.

Moreover, this report does neither deal with all AML issues nor does it comprehensively address all aspects of the AMLD.\textsuperscript{17} Notably, it does not deal with the notions that do not appear as broad and indistinct but as rather narrowly and clearly defined, e.g., PEPs. Furthermore, it does not address aspects that have extensively been dealt with by other authors, e.g., the risk-based approach (RBA).\textsuperscript{18}

\textsuperscript{16} Cf also chapter 5.
\textsuperscript{17} For a comprehensive overview of the AMLD, its framework and enhancements see Met-Domestici A (2016) The fight against money laundering in the EU: The framework set by the fourth Directive and its proposed enhancements.
2. Money Laundering – An Introduction

2.1. What is Money Laundering?

Money laundering is the process of disguising illegally obtained assets, making them appear as legitimate assets. Money launderers want to disguise the origin of funds that are found in criminal activity. They want to enjoy the profits without having to deal with the illegal past. In essence, money laundering is the process of making dirty money look clean.

Money laundering was originally associated mainly with drug trafficking and other forms of large organised crime. With such crimes generating big profits, there is a significant incentive to launder the funds. However, since money laundering is illegal it is not included in official economic statistics. Accordingly, the size of global money laundering can only be estimated. The International Monetary Fund (IMF) has estimated that the aggregate level of money laundered annually is 2-5% of the world’s gross domestic product, i.e. amounting to trillions of US Dollars.\(^{19}\)

Today, the main international actors in AML policies are:

- The United Nations (UN)
- The Financial Action Task Force (FATF)
- The Egmont Group, an informal network of national financial intelligence units (FIUs)
- The European Union (EU).\(^{20}\)

2.2. Money Laundering and the AMLD

Instead of using one single definition, the AMLD describes various aspects of money laundering. They all relate to intentional conduct:\(^{21}\)

“…the following conduct, when committed intentionally, shall be regarded as money laundering:

(a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person’s action;

(b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;


\(^{21}\) Article 1 AMLD.
(c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;

(d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c).

4. Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country. (…)

6. Knowledge, intent or purpose required as an element of the activities referred to in paragraphs 3 and 5 may be inferred from objective factual circumstances.22

The above definition is almost identical to the definition of money laundering enshrined in the UN Convention against Transnational Organized Crime23 and the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.24

2.3. The Money Laundering Cycle

At the beginning of money laundering is a criminal activity. The persons involved seek to control the generated funds without drawing attention to the criminal activity or themselves. The funds can consist of assets derived for instance from drug trafficking, insider trading, robberies or tax evasion. The criminals do this by disguising the sources, changing the form of the assets, and/or moving them to foreign places. Ideally, the paper trail back to the initial criminal activity is eliminated and the assets appear as legitimately acquired.25 The cycle of money laundering comprises three stages: 1. Placement; 2. Layering; 3. Integration.

22 Article 1 AMLD.
2.3.1 Placement Stage

Mr X robs a bank. To enter the financial system, Mr X deposits smaller sums into several bank accounts using different financial institutions to avoid legal thresholds that might trigger reporting requirements.

In the Placement stage, the proceeds of a criminal activity are introduced into the financial system. This first stage serves two purposes; it relieves the criminal of holding and guarding large amounts of cash and it places the money into the legitimate financial system.

During the Placement stage, money launderers are the most vulnerable to get caught since placing large amounts of money into the financial system may raise suspicions. Therefore, the Placement stage regularly involves: breaking up large sums into smaller amounts thereby bringing it under a given reporting threshold, sending funds across borders to deposit them in a foreign legal system, and / or purchasing high-value goods, which can be rather easily resold and thus converted into cash that appears to be of legitimate origin.\(^\text{26}\)

The process of Placement can be carried out through manifold activities such as:

- *Asset purchase*: The purchase of assets with cash is a classic money laundering method. The major purpose is to change the form of the proceeds from conspicuous bulk cash to some equally valuable but less conspicuous form (e.g., real estate);

- *Blending of funds*: A good place to hide cash is with a lot of other cash. Therefore, financial institutions may be vehicles for laundering. An alternative is to use the money from illicit\(^\text{26}\)

activities to set up front companies. This enables the funds from illicit activities to be obscured in legal transactions;
- **Currency exchanges**: Purchasing foreign money with illegal funds through foreign currency exchanges;
- **Currency smuggling**: The physical movement of illegal currency or monetary instruments over the border. The various methods of transport do not leave a discernible audit trail;
- **Gambling**: For instance placing bets on sporting events;
- **Loan repayment**: Repayment of loans or credit cards with illegal proceeds.\(^{27}\)

### 2.3.2 Layering Stage

Mr X wants to separate the illicit money from its source and thus transfers the funds to different onshore and offshore bank accounts.

In the Layering stage, the illicit funds are separated from their source. This is often done by a sophisticated layering of financial transactions that obscure the audit trail and removes the link to the original criminal activity. The Layering stage is the most complex and often entails an international movement of the funds. When the money launderer transfers proceeds through several jurisdictions and changes the format of the funds, it can be very difficult to trace the origin as well as the final destination of the proceeds.

Examples of activities applied in the Layering stage include:

- **Corporate accounts**: The transfer of funds through a series of corporate accounts where the beneficial ownership is hidden (e.g., by way of trusts or shell corporations);
- **Electronic fund transfers/wire transfers**: The use of multiple electronic fund transfers through bank accounts in numerous countries, with the launderer making use of accounts held in jurisdictions where anti-money laundering standards are low;
- **High-value goods**: The reselling of assets purchased during the Placement stage;
- **Investments**: Further investment of funds into tangible assets such as real estate or in legitimate business activities; and
- **Monetary instruments**: Conversion of deposited funds into monetary instruments such as cheques and money orders.\(^{28}\)

---


2.3.3 Integration Stage

The money returns to Mr X, appearing to be from a legitimate source. Mr X buys real estate to invest his laundered money.

In the final stage of the money laundering cycle - the Integration stage - the proceeds return to the money launderer, appearing to be from a legitimate source and the result of normal business activities. The laundered proceeds are now fully integrated into the financial system, making it difficult to distinguish legally and illegally obtained funds. The criminal can use the proceeds for any purpose.

Money laundering is not necessarily a complex process. However, for a money laundering scheme to be successful, the paper trail needs to be eliminated or at least it should consist of complex financial transactions that effectively make a detection unlikely. The number of steps taken to launder proceeds of criminal activities depends on the distance that the money launderer wants to put between the initial criminal activity and its proceeds on the one hand and the laundered assets on the other.29

The following figure illustrates different scenarios in the three stages of the money laundering cycle.

---

<table>
<thead>
<tr>
<th>Placement</th>
<th>Example 1</th>
<th>Example 2</th>
<th>Example 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Illicit funds are deposited into the financial system or invested into high-value goods.</td>
<td>Paying cash into a bank (potentially blended into funds from lawful activity).</td>
<td>Smuggling cash out of the country.</td>
<td>Purchasing high-value goods such as art, precious metal, and real estate or investment into business activities.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Layering</th>
<th>Example 1</th>
<th>Example 2</th>
<th>Example 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>The illicit funds are separated from their source, e.g. through financial transactions.</td>
<td>Transferring electronic funds across borders, often using shell companies or masking funds as proceeds from lawful business activities.</td>
<td>Depositing cash into account at a foreign financial institution.</td>
<td>Selling the purchased goods and assets for payments by cash, check or bank transfer.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Integration</th>
<th>Example 1</th>
<th>Example 2</th>
<th>Example 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>The illicit funds are retransferred to the money launderer in a changed format or as assets appearing to be legitimate.</td>
<td>Retransferring proceeds as repayment of (fictitious) loans or payments of (fictitious) invoices.</td>
<td>Transferring funds in a complex network of national and international transactions, which makes it almost impossible to trace the original source of the funds.</td>
<td>Re-integrating revenues from high-value goods, real estate, and business activities appearing to be legitimate into the financial system.</td>
</tr>
</tbody>
</table>

Figure 2: Money Laundering in Practice

The following concrete case shall serve as an additional example:

In the 1990s, Colombian drug cartels were laundering large sums of money through the purchase of life insurance policies in Europe, the United States and offshore jurisdictions. Using a small number of insurance brokers, Colombian drug cartels were buying investment-grade life insurance policies with cartel associates as beneficiaries. The policies were purchased with drug proceeds sent to the insurance companies via wire transfers and checks by third parties around the globe (placement and layering). The investigation revealed that the cartels were then cashing out these policies after short periods of time, despite the financial penalties invoked for early liquidation. The cartel beneficiaries would receive a check or wire transfer from the insurance company that appeared to be legitimate insurance/investment proceeds (layering). The cartels could then use...

these clean funds (integration). Investigation agents determined that the cartels had used this scheme to purchase at least 250 life insurance policies and launder some $80 million in drug proceeds.\textsuperscript{31}

3. Interpretative Guidance

3.1 “The Business Relationship Is Conducted in Unusual Circumstances”32

3.1.1 General Remarks

The wording of this risk factor arguably is the quintessential example of a broad and indistinct notion. Most gambling regulators or providers of gambling services are likely to ask themselves: What does “unusual” mean? And what does it mean in our industry?

A further challenge for regulators may be to translate “unusual” into the online gambling sphere specifically. It should be recalled that many jurisdictions have not yet regulated online gambling and their national authorities therefore have limited expertise regarding the remote gambling sector. Furthermore, contrary to land-based casinos, the online sector has been thus far much less on the radar of AML requirements.

Bearing these challenges in mind, I should emphasise that the regulators who have kindly agreed to participate in this study feature substantial experience in the regulation and supervision of the online gambling sector. Unsurprisingly, their answers reflect a profound understanding of the online sector and robust expertise in AML matters.

Having said that, the combined expertise of AML and online gambling is very likely to greatly vary between national regulators. Accordingly, some regulators may find the interpretative guidance offered by this report very helpful – while others may feel that they are already familiar with several of the presented aspects. The target audience of this report is broad: it shall serve most regulators as well as industry professionals as helpful guidance.

Two sections address each notion. First, a summary is provided of the regulators’ responses, that is, how they understood these notions and, if applicable, challenges that they identified from their perspective. Second, an interpretive guidance is offered that is informed by the various discussions with AML experts and the relevant literature. This regularly includes a discussion regarding the appropriateness of the wording and the scope of the risk factor at hand. The latter aspect shall assist gambling regulators in their own assessment of the risk factors and in considering and taking mitigating measures.

3.1.2 Gambling Regulators

One regulator held the view that “unusual circumstances” were situations in which the arrangement between the operator and the customer departed from industry standard. His definition of industry

32 Underlining emphasis and capitals added by the author in this title and all others relating to the presentation of the broad and indistinct notions.
standard is as unemotional as helpful: Industry standard is geared to make the most money while offering the level of services needed to retain the customers. Therefore, a regulator should consider it higher risk if an arrangement (or transaction or other circumstance) can be noted that seemingly does not favour profit but other factors (e.g., privacy). The regulator further argued that the word "unusual" did not serve particularly well to capture the very wide spectrum of risks among different gambling models.

Another regulator emphasised the role of the obliged entities (here: the providers of gambling services). It was for them to consider any situation outside of the norm. What could be unusual for one obliged entity may not be for another. For example, the circumstance that the customer relationship did not fit the operator's business profile or was at odds with the normal risk profile of the operator's customer base.

The regulator identified a difficulty in being asked by obliged entities to compose a list of unusual circumstances. Therefore, it was seen crucial to drive operators to understand the risks to their business and to enable them to identify what was unusual.

Another regulator saw a red flag where some aspects of the customer relationship or information provided by the customer did not fully reconcile with other data obtained or the usual course of action for that customer or similar customers (e.g., customer’s IP address did not match that of the identification data provided by the customer).

3.1.3 Who Should Define “Unusual”?  
3.1.3.1 The Legislator?

Before taking a closer look at the notion “unusual circumstances”, it seems appropriate to ask whether it was a bad thing that the EU legislator – and possibly national legislators as well – chose not to further define the notion “unusual”.

Who is entitled (powers) or most suitable (expertise) to define what the “usual business circumstances” are? The notion usual circumstances may regard business dimensions such as the location, allocated time, chosen means, practiced modes of contact and so on. Where a legislator does not have in-depth knowledge of a sector (and this will be regularly the case), there is the risk of a narrow and undifferentiated view on the business sector. As a result, the view on “usual” may be somehow sclerotic and, as a consequence, anything deviating from this view is likely to be seen as “unusual” and thus suspicious. Yet, from a business perspective there may be a perfectly sound explanation for the behaviour.

Accordingly, while the legislator (or the government through its administrative units) may have the powers to define “unusual circumstances”, it is arguably not the most suitable body to do so. If a public authority were to get involved in this definition, it would seem logic that only an authority with specialised expertise on AML (and gambling regulation) would be suitable to define “unusual” in the context of gambling services. Depending on the share of tasks in a given jurisdiction, this may
be the gambling regulator, the supervisory authority for financial and non-financial services, the financial intelligence unit (FIU) or other authorities.

From this perspective, it was after all not a bad thing but a sound choice that the legislator did not try to define “unusual” in relation to all business sectors once and for all.

3.1.3.2 Nullum Crimen et Nulla Poena Sine Lege

There is second point that should be made in relation to “unusual circumstances”. It regards fundamental principles of criminal law. As long the broadness of the notion “unusual circumstances” relates to obligations under administrative law exclusively, it may appear as acceptable. However, the broadness becomes problematic where the failure to comply with due diligence obligations is subject to sanctions under criminal law (or sanctions of criminal law-like nature).

The principle of legality is an essential achievement of the Enlightenment: Nullum crimen sine lege. Nulla poena sine lege. Conduct can only be regarded as a crime if the legislator has defined it a formal law. Sanctions shall not be imposed on anybody without that being defined in a formal law. Nulla poena sine lege certa means that the sanctions must relate to conduct that is defined by sufficiently precise wording. Nulla poena sine lege stricta means that the judicial interpretation of criminal conduct cannot go beyond the very wording in the law. Sentencing by analogy for instance is not permitted.

This fundamental principle has arguably been adopted in most jurisdictions based on the rule of law. And it has found express recognition as well in international criminal law, notably by the founders of the International Criminal Court. Moreover, the Court of Justice of the EU has made it clear that it is willing to uphold pan-European fundamental principles even at the cost of less effective (secondary) EU law.

As a consequence, it seems appropriate that courts as well as regulators that dispose of sanctioning powers of criminal (or criminal-like) nature apply restraint in passing sentences on

---

33 von Feuerbach (1801). Lehrbuch des gemeinen in Deutschland geltenden Peinlichen Rechts.
34 Rome Statute of the International Criminal Court of 17th July 1998:

**Article 22 - Nullum crimen sine lege**
A person shall not be criminally responsible under this Statute unless the conduct in question constitutes, at the time it takes place, a crime within the jurisdiction of the Court.
The definition of a crime shall be strictly construed and shall not be extended by analogy. In case of ambiguity, the definition shall be interpreted in favour of the person being investigated, prosecuted or convicted.
This article shall not affect the characterization of any conduct as criminal under international law independently of this Statute.

**Article 23 - Nulla poena sine lege**
A person convicted by the Court may be punished only in accordance with this Statute.”
individuals who have failed to detected “unusual circumstances”. Unless of course the national
criminal law and/or gambling regulation defines these circumstances sufficiently clear and precise.

3.1.3.3 Who Is Able to Define “Unusual”: Regulator or Obliged
Entity?

A gambling regulator may find it a challenging if not an impossible endeavour to specify towards
operators a detailed list of unusual circumstances. Similarly, the obliged entities may find it
challenging to recognise all such instances. Does the regulator have a duty to give guidance?

From a business perspective it is understandable that obliged entities reach out for guidance from
their regulator. As in relation to other regulatory issues (e.g. prevention of problem gambling or
fraud), serious operators want to be compliant with the law. No sensible operator would
intentionally seek reputational damage. Since many regulatory authorities also have powers to
sanction non-compliant behaviour, the obliged entities will feel more comfortable when they know
the regulator’s expectations with regard to AML compliance. The most convenient would be a
detailed list that would allow to “ticking the boxes”. Complex compliance work would thereby be
rendered significantly easier.

By contrast, several of the interviewed experts as well as gambling regulators shifted the duty of
interpretation of “unusual circumstances” towards the obliged entities.36 The rationale for this is that
the operators were in the best position to assess what unusual behavioural and transactional
patterns were. It was them who knew the normal business circumstances – and could therefore
recognise the outliers.

There may be a further reason for the reluctance of regulators to provide guidance: an operator
against whom an investigation is opened for non-compliant AML practice would be likely to
confront the regulator with the latter’s guidance, notably when the guidance did not list the
constellation at hand among the unusual circumstances.

3.1.4 How Can Obliged Entities Detect the “Unusual”?

For the purpose of this study, I shall define “unusual” as follows:

Business circumstances, customer behaviour and transactions are unusual when there is a
discrepancy between what can normally be expected based on the customer profile and what is
actually observed in practice.

To illustrate: Based upon initial information a customer is expected to gamble regularly by wagering
limited amounts but features a very different behavioural pattern. For instance, the customer

---

36 Even where gambling regulators have chosen to provide further guidance to operators, this has normally regarded
aspects other than defining „unusual circumstances”. Cf. e.g. Financial Intelligence Analysis Unit Malta & Malta Gaming
Authority (2017) Consultation Document: Application of Anti-Money Laundering and Countering the Funding of Terrorism
obligations to the Remote Gaming Sector.
makes a large payment on the player’s account, hardly uses his account over a long time, and then withdraws the money.

Obliged entities therefore need to put in place effective policies, programmes, procedures and systems to give meaning to these two dimensions:

a) What is the expected customer behaviour (customer profile) and

b) What is the observed customer behaviour (monitoring).

### 3.1.5 Customer Profile

#### 3.1.5.1 KYC: Yes. But also “KYB”!

Assessing money-laundering risks requires sound judgement and is not an exact science. Yet, a systematic and structured approach to AML allows obliged entities to apply their judgment on safer grounds of manoeuvring.

The first step in detecting the unusual is to define the usual. Obliged entities should draw a customer profile for each customer. The profile contains information on the behavioural patterns that can normally be expected from this customer. What is usual, normal or customary may vary depending on the customer’s background, his occupation, the types of products and services he uses, etc. Developing an accurate customer profile is important in managing AML risks. In view of this profile, the obliged entity requests information from the customer (identification and additional information) and where appropriate verifies the information. These steps are notorious under the notion KYC: Know Your Customer. KYC is an ubiquitous term among AML professionals. It essentially means that an obliged entity must have a sufficient understanding of its customer.

Yet, KYC is not enough. KYC has to go hand in hand with “KYB” – the relevant staff members must have a sufficient understanding of their company’s business, including product portfolio, customers and payments involved. Defining the expected conduct in relation to customer accounts requires a true understanding of the gambling field that the obliged entity is active in. Only then the staff in charge for KYC and monitoring will be able to notice the outliers.

According to one expert, banks (at least in some countries) systematically categorise their clients. Among other parameters, a 24h transaction threshold is defined for each category – if transactions pass that threshold a red flag is raised. It is then expected from the monitoring officer to look in more detail into this matter and whether the outlier can be explained.

In short, a precondition for an effective and meaningful monitoring is the creation of a sufficiently detailed customer profile that is complemented with red flags (e.g., thresholds). Appropriate KYC compliance also requires the customer profile to be updated. This should be done continuously whenever existing customer information changes or new relevant information becomes available.

---

Unusual circumstances will then mean that they deviate from a behaviour that would be expected based on the customer profile.

3.1.5.2 Profile Contents

We have defined “unusual circumstances” as situations featuring a discrepancy between what can normally be expected based on the customer profile and what is actually observed in practice. The very definition illustrates the importance of an accurate and sufficiently comprehensive profile: best monitoring practices are worthless if not combined with a carefully drafted customer profile.

What does customer behaviour include? The customer’s behaviour includes all his transactions, his play, and his communication. These factors may not only serve to analyse AML risks but also problem gambling risks.

What information should be included in the customer profile to allow for effective AML compliance, including meaningful predictions as per the customer behaviour? Again, regulatory practices in the financial sector can be used to inform gambling regulation. The FMA Due Diligence Ordinance in Liechtenstein defines the expected contents of customer profiles.38 We shall adopt here those elements, which can also be meaningful in an online gambling context.

- The customer
- The beneficial owner; this seems particularly indicated where accounts relate to legal persons
- The organs and third persons holding a power of attorney
- Economic background of the person, including job and business activities
- Likely origin of the money to be transferred to the player’s account
- The transfers should normally serve the player’s gambling activity; should the player request or his behaviour express other purposes this is to be noted.

How detailed should this information be? The RBA demands a differentiated scheme. Certainly, there should be a minimum stock of information imposed by internal procedures. What is more, the riskier a business relationship is seen by the obliged entity the more information and the more detailed information it must collect.

There is another indicator for the appropriateness of the customer profile: third party AML professionals – for instance FIU or regulator staff - must be able to make sense of the profile without much effort. Where a specific transaction is being inquired the external experts must be able to swiftly compare the monitored behaviour with the customer profile and be enabled to identify anomalies.

38 Article 6 Due Diligence Ordinance.
3.1.6 Monitoring

The customer profile only forms the starting point of CDD. The business activities are then to be monitored by specialised staff. Any “unusual activities” must be detected in this phase of CDD and then appropriately processed. This regards any situations, which are discrepant and anomalous from the customer profile.

Part of the monitoring process is also the updating of the customer profile. The frequency of this exercise will depend on the specific AML risk allocated to the customer account. A minimum frequency should be defined internally for all accounts. Any relevant changes must be integrated in the profile. This may include information gathered directly from the customer or information sought by the obliged entity from third party service providers.

Red flags can be used to indicate unusual customer behaviour. Staff members may place a red flag where they become aware of circumstances in their contact with the player (e.g., the player suddenly accesses regularly the website from a different world region that may be linked to drug trafficking) or where flags are set automatically (e.g., player wagers above a certain predefined threshold).

Where unusual transactions or circumstances are detected they must be inquired. Predefined procedures and protocols are key in this exercise. Implementing CDD by flying by the seat of one’s pants is not advisable if only because it must be clear and unambiguous to external experts (e.g. FIU) how the obliged entity reacted to the situation, what measures it has taken and how fast it has taken them.

Where the staff member cannot make sense of the detected situation he must escalate the issue to the competent AML officer on duty. In the banking world, this may happen as follows:

A monitoring staff member notices that a civil servant receives a high amount of money on his bank account. The money is not transferred by his employer but by an unknown third party; the amount is above the normal financial means of that customer. The monitoring officer reports the issue to the staff in charge of that customer account. Maybe doubts can be cleared swiftly: for instance the customer may have inherited a large amount of money, communicated this to the bank in advance and the name of the sender of the transaction backs up the story. Where no sensible reason can be recognised the matter must be further inquired and eventually reported to the FIU.

Another unusual circumstance in the banking sector arguably is if a walk-in customer requests to deposit a large amount of money without that customer having had any relationship to the bank earlier.

39 Cf. also the wording in the Swiss AML Act, Article 6 lit. a. “The financial intermediary must inquire the background and the purpose of a transaction or a business relationship, if: a) the transaction or the business relationship appears unusual, except if its lawfulness is recognisable.”
The monitoring exercise must be adequate to the risk, in other words: player accounts associated with higher risks have to be monitored continuously. They should also be monitored tighter than low risk accounts. In keeping with the RBA, regulators and FIUs are unlikely to impose specific frequencies of controls. In any event, in the online gambling world that features countless business transactions even within just an hour, the monitoring exercise will normally be continuous, at least in terms of red flag alerts popping up based on certain parameters.

As in any continuous exercise one danger lies in neglects due to routine. Of course, good compliance work also requires standard procedures and protocols that staff respect. Yet, where obliged entities implement AML compliance as a mere mechanical routine, there is a good likelihood that some money laundering risks will remain undetected as they stay under the radar. It is preferable to trust trained staff and leave them some discretion in assessing a situation, which also requires of course a sound level of expertise. Moreover, common sense is required as each business relationship may feature its individual characteristics.

Where additional CDD inquiries seem indicated, the compliance officers have to gather the necessary additional information and to verify its plausibility. The information is relevant if it allows the person in charge to make a robust background check. All additional documents and the conclusions must be duly recorded and filed (recordkeeping). Where the AML officer in charge identifies a higher risk situation and cannot make sense of the transfer, behaviour or similar, he will have to submit a Suspicious Activity Report (SAR) to the national FIU (and / or regulator depending on the national law).

3.1.7 Unusual Higher Risk Behaviour: Experiences from the Financial Sector

It is often assumed that remote gambling channels would be more prone to money laundering than land-based gambling. And at the same time neglected that remote channels offer technical possibilities that are not available in the terrestrial sphere. Similar fears of technology can be observed in relation to other compliance issues, too.

Online operators have the technical possibilities to define the parameters that flag “unusual behaviour”. In doing so, they can find inspiration from business sectors that have built long-standing experience in AML compliance. The financial market is such sector. The Swiss Financial Market Supervisory Authority (FINMA) defined a long list of potentially unusual higher risk constellations. Obliged entities subject to FINMA’s jurisdiction must take them into account. While these constellations are mainly steered towards the financial sector, they can nevertheless offer useful indications for the gambling sector, too. In the following these constellations have been adapted to scenarios relating to gambling customers (to the extent possible):

40 Articles 27-29 Due Diligence Ordinance.
41 For a paper that counters many of these assumptions see Levi M (2009) Money Laundering Risks and E-Gaming: A European Overview and Assessment.
43 Art. 12-13 FINMA Money Laundering Ordinance.
- Higher risks are potentially present where transactions take place for which no economic purpose is recognisable or transactions that simply do not make economic sense (pt 2.1.1 i.f. of the Ordinance). The same may be true in relation to company structures in a business relationship that are without economic sense. By contrast, legitimate tax savings / optimisation can make economic sense.

- Shortly after the reception of payments on the player's account these assets are withdrawn without any plausible reason in view (pts 2.1.2 and 3.2.14); this may also include prior minimal gambling activities.

- The customer wishes to transfer money to another player's account or to a bank account of another customer. But it becomes clear that he does not want to fully disclose all identification details of the recipient (3.2.4). Similarly, if somebody else is attempting to send money to a player's account and does not properly identify himself (3.2.7) or even requesting that the customer should be paid out in cash (3.2.8), which in principle would be possible if the physical gambling premises host online gambling services, too.

- Many persons make or attempt to make payments to the same player's account (3.2.11).

- The customer does not fit the usual customer base of the operator, in other words: why did the customer then choose this operator (2.1.3)?

- A largely inactive account suddenly becomes heavily used (i.e., frequency or amounts) without there being a plausible reason available (2.1.4; 3.2.2).

- Transactions, which are at odds with the experiences of the operator with this customer and the nature of this business relationship (2.1.5).

- A customer has provided false or deceptive information or has refused to provide information and documentation without plausible reason. These would need to be situations in which it is normal and necessary to ask for the information / documentation (2.2).

- Regular payments from high risk countries or payments to countries that are in the vicinity of countries hosting terrorist groups (2.3) and high and frequent payments to drug producing countries (3.2.9).

- A customer attempts to avoid - even duly announced - personal contact intended by the operator (3.4.1).

- A customer wishes to close an existing account and wishes to not leave any paper or electronic trail; at the same time, he opens a new account for himself or his relatives (4.1).

- A customer wishes to be provided with receipts of pay outs that were not produced in relation to these amounts or that would be in any other way inaccurate or not according to the normal procedures (4.2) or who wishes to have such payments sent by indicating a different person ordering the payment, e.g., an alleged financial surprise gift for the chosen third person (4.3).

- There are known prosecutions against the customer in relation to felonies, corruption, abuse of public money or qualified tax crimes (4.6); in my view, the same should apply to fraud-related felonies due to the relevance of fraud-related compliance work in the gambling industry.
3.1.8 Higher Risk: Are There Abstract Early Indicators?

We have defined the notion unusual by contrasting the initially composed customer profile with the actual customer behaviour as it is monitored over time (i.e., play, transactions, communication). It may take time until a red flag is raised indicating a potential unusual behaviour.

The question is whether there are indicators in the (online) gambling sector that early on or even from the outset point at unusual circumstances. A FATF report suggested such constellations and we shall discuss them in the following. In my view, they should be applied with the necessary caution. An obliged entity should not look at these circumstances as reliable indicators. The reason lies in the very nature of the RBA: The risk assessment always has to take place in relation to the concrete case. It is not an abstract exercise.

As per limitations, it was noted that this report focuses on offering guidance in relation to broad indistinct notions. It does not deal with other risk factors, which appear to be sufficiently clear and defined. This is for instance the case with regard to Politically Exposed Persons (PEPs). People qualifying for that category are duly defined in the AMLD and the FATF recommendations.44 Similarly, customers may have links to world regions that are associated with geographic / country-specific risks. Operators are well advised to consult a variety of credible and reputable sources.45 Some supervisory authorities may interpret the mere residency of the customer in an "offshore" destination as higher risk.46 Another indicator of geographic risk can include a situation where the IP address used by the player does not match the geographic residency that he declared. Finally, another higher risk indicator could be seen in a significant geographic distance between the seat of the obliged entity and the residence of the customer without a recognisable plausible reason.47

By contrast, the following risks relate to the customer and early behavioural traits. Even though FATF composed them having mostly land-based gambling in mind, we can discuss to which extent they may be relevant for the online sector, too.48

- High spenders: Given the differences between the many providers of gambling services and their respective customer bases, what can be considered “high spending” is likely to vary from one operator to another. What is more, the relative purchase power and value of the wagered money in the country of residence should be taken into account. The difficulty

---

44 FATF recommendations (2012), p. 120: FATF defines PEPs as “individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories”. The risk factor PEP is not phrased in broad and indistinct notions and hardly raises questions as per interpretation. It is therefore not further dealt with in this report.

45 The financial industry has established good practices in this regard, relying for instance on sanctions lists and intelligence services. Such information reaches from official sanction lists of international or national bodies to information gathered by non-governmental organisations or companies specialising in such services (e.g., corruption and fraud levels, terrorist organisations).

46 Österreichische Finanzmarktaufsicht (2011) Rundschreiben zum risikoorientierten Ansatz, p. 32. The term offshore is problematic: cf. pt 3.2.4.


for the operator will be to define the relevant time frame: does high spending relate to one
session, several consecutive sessions or over a longer period of time?

- However, operators arguably already have made this definition work and identifying high
spenders for AML purposes should be effortless. The reason lies in well-established and
practised customer policies in regard to high spenders. It is very common to apply loyalty
programmes, bonuses and special marketing towards high spenders.\textsuperscript{49}

- Disproportionate spenders: An obliged entity can only come to this conclusion if it disposes
of the necessary information and documentation regarding the customers’ financial
resources. Only where an operator has knowledge of the likely income and assets of a
player does it have the possibility to assess the (dis-)proportionality of the spending. In
some jurisdictions, operators may be under a regulatory requirement to collect such
information but mostly it will be a risk-based decision by the operator to seek that
information.

- In practice, the difficulty consists in the fact that many customers are unlikely to appreciate
detailed inquiries into their finances by a private entity. All the more when this comes from a
company, which they had thus far experienced as discreet and keen to respect privacy and
data protection.\textsuperscript{50} It can be challenging communication-wise to seek financial information
from the customer.

- Operators, however, may also be able to draw tentative conclusions from more easily
available information (e.g., occupation, marital / family status, self-declared intended
spending or self-imposed spending limits); some of this information being verifiable by
Internet searches.

- Casual (irregular, rare) customers: This circumstance does not say much in relation to a
concrete risk. The relevance of this rather relates to the monitoring exercise: the spending
patterns of irregular or rare customers are more difficult to identify. Accordingly, it is also
more difficult to define outliers.

- One pattern that an obliged entity may see as higher risk could consist in a customer who
rarely engages in gambling but when he does, he does so with large amounts.

- Improper use of third parties: a money launderer may use other persons to gamble for him,
breaking up large amounts into smaller wagers to avoid thresholds above which CDD would
apply (”smurfing”). Behind the scene transfers are difficult to detect, be it in the land-based
or online sector.

- Junket operators: This could be perceived a risk in the online gambling sphere if the tour
operators brought tourists to a land-based venue in which people can also gamble online,
for instance in a separate VIP private room. Junket operators typically pool the wagers of
the individual customers.

- Multiple accounts by one player: Some players may try to open several accounts with one
operator. A motivation behind this could be to hinder the operator to track their aggregate
gambling activities. They could thereby obscure their overall spending with that operator.
What an operator in any event cannot identify is the overall spending of the player with
other operators.


\textsuperscript{50} These issues are relevant also in other industries: Stämpfli AA (2009) Kundendaten von Banken und
Finanzdienstleistern.
- Operators should thus make sure to detect accounts with similar players’ names and similar physical descriptions (e.g. age, male or female, eye colour, hair colour, height, weight).
- Unknown Customers: this circumstance reminds of the constellation regarding irregular customers. Unknown customers have not featured yet gambling patterns. A higher risk could certainly be seen where an unknown customer purchases gambling currency (points, chips, etc.) for large amounts of money, however, engages subsequently only in minimal gambling or no play, and then has his gambling currency paid out in real life currency.

3.1.9 Higher Risks Through Transactional Circumstances

The thus far described unusual circumstances have related to monitored behaviour not matching the customer profile as well as to abstract early indicators (e.g., irregular customer). In addition, there may be transactional circumstances that appear as unusual.51

- Mixed gambling chains
  Payments to providers of online gambling are regularly made through the financial industry, i.e. credit card payments, bank transfers, etc. In some cases, however, online channels may operate as part of mixed gambling chains that include land-based casinos, betting shops and other venues. The higher risk stems from the circumstance where customers can make cash payments in land-based outlets, which then can be credited to their online accounts as well. In such constellation, CDD measures must be taken, e.g., ID check to ensure the depositor is indeed the account holder.
- Transfers between customer accounts
  Where the regulation in place permits online providers to allow for inter-account transfers between different customers, such transfers will have to be carefully monitored and a robust audit trail must apply. For example: If the IP address of the sender matches the IP address of the receiver, this should raise questions since the transfer was supposed to go to another customer (and therefore likely to another IP address).
- Multiple accounts / wallets: It goes without saying that an obliged entity will have to monitor the customer’s aggregate behaviour across its whole product line. Relevant for the conclusions to be drawn is the full picture, not just for instance the gambling behaviour relating to one product (e.g., poker). Such situations may include mixed gambling chains, multiple websites owned by the obliged entity or one website offering a range of different types of gambling. Where customers try to open several accounts, they may be trying to obscure spending levels or thresholds above which enhanced CDD automatically apply.
- Account changes
  Customers often make their payments through one bank account in order to gamble online. But they also often hold several financial institution accounts. Where a customer wishes to change the applicable account, the obliged entity should look into the matter and clarify the reasons.
- Platform not operator
  Where the operator itself does not own the online platform but it is shared by several

operators, it is important to have clear responsibilities as per AML obligations. Patterns that should be inquired include for instance chip dumping in peer-to-peer games (e.g., poker).
3.2 “Legal Persons or Arrangements that Are Personal Asset-Holding Vehicles”

3.2.1 Online Gambling Regulators

One regulator noted that this risk factor was unlikely to apply to the customer base of gambling operators. The statement expresses the view that gambling customers are natural persons, i.e., human beings. Yet, as another regulator noted this risk factor can apply in the gambling world.

The starting point is that some jurisdictions at least permit that any “person” (natural or legal) can sign up as a gambling customer. This is only then not the case if the gambling regulation of the licensing jurisdiction prohibits the acceptance of legal persons or if the company applies such policy in spite of it being legal to accept legal persons in that jurisdiction.

Certainly, the normal case is that a gambling customer is a natural person. But it is nevertheless worth looking into this risk factor, too, as it can occur in practice. Bearing in mind the earlier mentioned category of “unusual circumstances”, it would in fact seem all the more appropriate to consider this risk factor in the gambling world, exactly because it regards an “unusual” customer base.

One regulator added that personal asset-holding vehicles should only be seen as a flag that may indicate higher risk. This element, however, should only form one aspect among others to be considered in a more comprehensive and complex AML analysis.

3.2.2 Tax Crimes

The AMLD introduced tax crimes to the list of predicate crimes. This has broadened the scope of application of AML rules significantly. Essentially, transfers of undeclared assets (tax evasion) can potentially be seen as money laundering, i.e., as an attempt of disguising the predicate crime.52

In line with this, one expert expressed the view that this risk factor must have been adopted in the context of the fight against tax crimes. What speaks for this motive is the very wording of the provision and how it differs from another broad and indistinct risk factor:

“the ownership structure of the company appears unusual or excessively complex given the nature of the company's business”.

This latter risk factor refers to the nature of the business at hand and how the ownership company does not make economic sense (e.g., too complex for this business; too costly as a network of companies). By contrast, the factor “legal persons or arrangements that are personal asset-holding

vehicles” does not mention complex business structures that do not make economic sense in relation to that person and business.

Most of the experts agreed that the notion personal-asset holding vehicle referred to arrangements such as foundations and trusts. Essentially, domiciliary companies or similar arrangements can serve to hold personal or family assets. One person also mentioned bearer bonds.

It may be tempting to instantly think that the mere presence of such legal persons or arrangements was a clear indicator for predicate crimes such as tax fraud. Yet, they may simply serve to legitimately lower the tax burden. Two questions can be asked in this context. First, is the arrangement legal or illegal? This will need to be assessed on a case-by-case basis in the light of the applicable national tax statutes and case law. Second, is the arrangement ethically sustainable? It may well be the case that an arrangement is legal but not ethically sustainable in the public opinion. For an average natural person, i.e., taxpayer, it is certainly hard to understand when a large successful company pays virtually no taxes at one of its establishments.

Accordingly, it is not surprising that the subjective perception of personal asset-holding arrangements varies significantly, even among the interviewed experts. To illustrate: one professional argued that the question must immediately be asked why a natural person does not hold assets on his own person and account. Accordingly, such arrangements had to be fishy. On the other hand, another expert noted that such arrangements were not per se problematic. Simply, the national governments should assess the company structures available under their national laws and understand the respective risks of their legal arrangements.

3.2.3 What Does “Domiciliary Company” Mean?

Various legal persons and arrangements can be summarised under the notion “domiciliary company”. Domiciliary companies essentially do not operate a commercial business. They may for instance administer the assets of related companies. The FINMA Ordinance uses the following definition:

“Domiciliary companies: legal entities, companies, institutions, foundations, trusts, fiduciary companies and similar associations that do not operate a trading, manufacturing or other commercial business. (…)”

According to Article 13(1) of the Ordinance, any financial intermediary (i.e., obliged entity) shall develop criteria that flag a high-risk business relationship. Article 13(2) suggests among other criteria: complex structures, especially the use of domiciliary companies. The provision further notes that such companies typically lack own premises and staff. When confronted with a domiciliary company, the obliged entity must obtain a written declaration that states the beneficial

54 Article 2 a. FINMA Money Laundering Ordinance.
owner. Effective CDD measures help to avoid typical typologies in relation to false or falsified beneficial ownership.

3.2.4 What Does “Offshore Company” Mean?

The notion “offshore” is an extremely frequent notion in media and politics. It is often used in the context of domiciliary companies. There is an interesting phenomenon to this notion: while it is in permanent use, its definition is unclear. And while many jurisdictions quickly call others “offshore”, none likes to be referred to as offshore.

The use of the notion offshore does regularly not reflect an unemotional intention. Often it is referred to with a political agenda or clear personal view in mind. Depending on the exact political narrative, offshore can mean “an island” or “outside of the EU” or simply “anywhere outside the US” – in other words, it reflects an arbitrary judgment. It is therefore a very imprecise and thus unsuitable term to address the issues at hand.

As an example, the MONEYVAL report 2013 uses this notion without an actual attempt of defining it. Similarly, the notion “illegal” is often used too lightly considering that it refers to something severe, a criminal act. The two are often combined:

“and to prevent the provision of illegal gambling, which, as was reported, generally originates from offshore jurisdictions or certain Asian countries.”

From a more unemotional viewpoint, the term offshore often refers to the fact that certain company activities have been outsourced or offshore, i.e., certain services, notably financial services, are provided in these jurisdictions to non-residents.

3.2.5 What Does “Shell Company” Mean?

Besides offshore and domiciliary company another term is frequently used: shell company. Shell companies regularly feature limited liability (Ltd), are not publicly traded, have typically no physical presence other than a mailing address and generate little independent economic value. Nevertheless, shell companies can be set up by individuals and legal entities for legitimate purposes, such as to hold stocks or intangible assets of another business entity or to facilitate

---

55 Article 63 FINMA Money Laundering Ordinance. It is noteworthy that Swiss banks do not accept trusts as contracting partners, only the trustees who must identify themselves as natural or legal persons: cf. Article 16 of the Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (2015) as well as the Commentary on the Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (2016).
56 Cf. the typologies in MONEYVAL (2013) The use of online gambling for money laundering and the financing of terrorism purposes, p. 10-11, bullet points 6 and 8.
57 MONEYVAL (2013) The use of online gambling for money laundering and the financing of terrorism purposes, p. 9. The expressions “unlicensed in the point of consumption country”, “unlicensed in the country of the company seat”, “illegal” and “punishable” all describe different legal constellations. They are often confused.
domestic and cross-border currency and asset transfers and corporate mergers. At the same time, such structures can be abused for money laundering purposes.59

One reason for their popularity is that these companies can often be easily and inexpensively set up depending on the jurisdiction. When the company’s seat is in a jurisdiction that hardly offers any legal aid to other countries, it can become virtually impossible for law enforcement authorities to unveil the ultimate beneficial ownership.

Contrary to conventional wisdom it is not necessary to go to a deserted island in the Caribbean to set up a shell company. Authors have described similar arrangements for instance in relation to mainland US. While all states have laws governing the establishment of limited liability companies, most states do not collect or otherwise require the disclosure of ownership information at the moment of establishment or after. Furthermore, there are several ways that are consistent with state laws, in which founders of shell companies can obscure company structure, ownership, and activities. For example, many state laws permit corporations, general partnerships, trusts, and other business entities to own and manage LLCs. This enables individuals or legal entities to further conceal involvement in the activities of a shell LLC. Layers of ownership can thus be devised, which makes it highly unlikely that the relationship among numerous individuals and companies can be identified, even if one or more of the owners are identifiable. Finally, shell companies can be abused for tax fraud by applying illegal loan schemes that do not reflect typical market loan conditions. If in addition the ownership structure is disguised as aforementioned the loans can be used without authorities realising that a person is actually borrowed his own money.60

Charities are another form of incorporations that have in more recent years come on the radar of AML and CFT policies. The relevant question there is whether the use of the funds reflects the purposes of the charity as enshrined in the deeds or whether some of the funds serve illegal purposes. Criminals can infiltrate a charity and deviate funds or even set up a charity with the very purpose to finance causes that can hardly be described as charitable. It is therefore important to have effective internal controls and external independent auditing in place to ensure that the charity’s funds and spending are fully accounted for.61

3.3 "The Ownership Structure of the Company Appears Unusual or Excessively Complex Given the Nature of the Company's Business"

3.3.1 Online Gambling Regulators

As a regulator pointed out the terms "unusual or excessively complex" are subjective. Looking at them as a potential high risk is nevertheless seen as sound provided it is used to trigger scrutiny rather than condemn the structure from the outset. Scrutiny may in fact reveal that a complex structure has its roots in tax efficiency or a history of mergers and acquisitions, i.e., legitimate business considerations and activities.

"Unusual or excessively complex" may involve: multiple layers of ownership, the use of ownership vehicles where ownership can be arbitrarily modified or structures embodying loans with non-payback conditions. Or more generally: corporate structures that stray from a simple company with single tier shareholders. A regulator argued that the risk is higher the more layers of ownership and the more exotic the structures are, particularly if they incorporate "moving parts" such as conditions, which once triggered cause ownership to change.

Another regulator argued that customers were predominantly natural persons in the i-gaming sector and therefore these types of complex corporate structures were unlikely to exist. Where a customer was a legal person, the magnitude and nature of transactions by themselves would in general necessitate higher levels of due diligence being undertaken. Accordingly, increased CDD was needed where such structures were to be found.

One regulator argued that this risk situation was more likely to involve gambling operators' business with third parties, i.e., B2B partners. Unusual or excessively complex could mean that a company structure did not offer any apparent legal, economic or commercial benefits. In short: no logical reason for the ownership structure is recognisable. The presence of such B2B partners would be an element that this regulator would want to examine when considering licensing applications of the B2C provider.

3.3.2 Legitimate Purposes for Complex Structures

Complex company structures or the presence of foundations and holdings in a company organogram really does not have to mean much. Several experts agreed with this view. One illustrated it with prominent examples. Some of the leading German and Swiss newspapers are predominantly or partly held by holding companies or foundations. Most people will arguably agree that the highly regarded newspapers “Süddeutsche” (Germany) and “Tages Anzeiger” (Switzerland) do not form part of the usual suspects of money laundering schemes. As noted earlier, reasons for such company structures may include the genesis of the company (e.g., mergers and acquisitions, diversification of the product portfolio) or legitimate motives of the owners (e.g., tax optimisation).
There is a further aspect: Assessing things exclusively from a Western (or national) perspective can be misleading. Living in the Western World regularly means to lead a safe life. And to take safety for granted. To illustrate: when you live on an “island of bliss” you may take for granted: political stability, monetary stability (hardly any inflation or deflation), well run and financed public schools, affordable and well-functioning health care system, and very low crime rates (e.g., hardly any robberies or kidnappings). From this luxury perspective it may appear as fishy if somebody does not want his name mentioned in his publicly known company; that person must be hiding illegitimate business.

Yet, life may look fairly different in another part of the world. Kidnappings for instance are notorious in some countries. Successful businesspersons in these countries have a very concrete interest in staying discreet about their success – or alternatively increase their security detail significantly with all the limitations for personal freedom, which this brings. The security concern regularly regards close family members.

However, as noted correctly by another expert, the security argument becomes non-plausible where the same person flashes his wealth in public. Similarly, intentional media appearances alone or with high-ranking politicians would not seem to serve the interest of discretion either. The consistency of the behaviour is therefore a good indicator in relation to this argument.

3.3.3 International Structures: Business as Usual?

An international company structure should not be seen as suspicious per se. All experts agreed on that view. A national political agenda that demanded (e.g. for tax reasons) to make international company structures more difficult might very well achieve the opposite, i.e., businesses moving abroad in their entirety. Larger international companies often have establishments in several countries through associated companies that they own. Internationality therefore is business as usual in company structures.

However, as normal as internationality is in business it is also sought after by criminals. The motive for money launderer to go international is to make law enforcement efforts very difficult. The hiding and disguising exercise becomes more effective when a network of companies is spread over numerous countries. Prosecutors will find it difficult to bring light into a complex structure in regard to its beneficial ownership when the companies are located in jurisdictions with which they do not enjoy agreements on legal cooperation. These legal hurdles can make it virtually impossible to investigate the facts.

62 The immediate past German ambassador to Switzerland referred to this Alpine Republic without any irony as an island of bliss: Neue Zürcher Zeitung, July 10th 2017, Otto Lampe: Leben in der Schweiz: Insel der Glückseligen.
3.3.4 What Is an Excessively Complex Structure?\textsuperscript{63}

The very notion "excessively complex structure" suggests that it is ultimately a subjective call whether something is seen as complex or even excessively complex. It would further seem that a moderate degree of complexity does not suggest higher money laundering risks but only an excessive degree of complexity.

What can be indicators of a complex structure? The Liechtenstein FMA proposed a series of factors that suggest the presence of a "complex structure".\textsuperscript{64} The FMA composed this guidance in relation to a primary law provision that requires enhanced CDD in the presence of complex structures, complex or unusually large transactions or transaction patterns that do not pursue an economic or legitimate purpose.\textsuperscript{65} Those structures should be regarded complex that hinder the transparency regarding compliance relevant information. The factors include:

- number of "underlying companies" involved in the structure
- number of jurisdictions involved in the structure
- involvement of jurisdictions whose AML measures do not correspond to international standards
- extent to which compliance relevant information is available from official registries or publicly certified documents.

It does not seem advisable to only look at one of these criteria. For instance, the number of jurisdictions involved does not say much by itself. All criteria need to be taken into account.

There can also be mediating factors that can be taken into account according to the FMA. Such mediating factor could be seen in the fact of the obliged entity having enjoyed long standing business relations with the company including frequent customer contact. Or if the obliged entity has substantial experience with the involved jurisdictions, namely their laws, regulations and supervision.

3.3.5 Disguising the Beneficial Ownership

One expert argued that a very long chain of companies may very well be an indicator for illegal activities and that he had come across a chain featuring approximately 50 companies. Another person noted that it was suspicious if a company was established and operating (only) in one country but part of an international company structure with wide geographic reach. It seems though that both factors are not reliable indicators in view of illegal activities. Companies can set up associated companies in various jurisdictions whose activities may focus on the respective national

\textsuperscript{63} The antonym of complex may also help to further clarify the notion. The Guernsey Financial Services Commission described in its handbook i.a. low risk situations, for instance businesses with a simple structure (p. 61, pt 197): "a locally resident retail customer purchasing a low risk product where the purpose and intended nature of the business relationship or occasional transaction is clearly understood by the financial services business and where no aspect of the business relationship or occasional transaction is considered to carry a high risk of money laundering or terrorist financing."

\textsuperscript{64} FMA Guidance 2013/1, p. 7.

\textsuperscript{65} Article 11(6) lit. a. Due Diligence Act.
market. What is more, a daughter company may buy shares of yet another associated company, for instance to streamline management policies between two markets.

In my view, attempts to define “complex” or “excessively complex” structures somehow fail to address the core issue. Coming back to what was noted earlier, the actual problem does not lay in complex company structures. There may be legitimate reasons for their existence. The core issue is the disguising of the beneficial ownership. The question is: Who benefits ultimately from all these companies, trusts and foundations? From an AML perspective a wide net of underlying companies is not problematic as long as the beneficial ownership is clear and not disguised.

One good indicator of higher risk really is when the structure does not make economic sense as this would go against the normal modus operandi in business: to make profit. This is well described in the FINMA Ordinance.

“Transactions bear a heightened risk of money laundering if:

their structure indicates an illegal purpose, or their economic purpose is not discernible or that (the structure) may even seem absurd from an economic point of view (…)"

Where a money launderer sets up company structures that serve one single overriding goal, i.e., disguising the beneficial owners at all price, it is likely that a careful investigation will conclude that the structure does not make economic sense. The criminal will then choose to create companies, foundations and trusts that create little economic value by themselves. What is more, the establishment and running of these arrangements create costs. Accordingly, their value solely lies in hiding things. Law enforcement authorities have found that opaque structures have been recurrently used in major money laundering cases to hide the beneficial owners.

One would be naïve to think that only certain sectors can be affected by such activities. In principle, all sectors can be infiltrated by organised crime and many supervisory authorities still have to develop a better understanding of AML risks to which their sector is exposed. Similarly, it is not an issue limited to certain jurisdictions or just one or two types of legal entities /
arrangements.\textsuperscript{72} It was suggested that the more techniques are used, the more cash can be successfully laundered.\textsuperscript{73}

When stricter AML regulation is passed and implemented in one sector, other sectors may become more attractive to money launderers.\textsuperscript{74} Smart perpetrators will follow logical considerations in identifying their most attractive money-laundering scheme. The question ultimately is: What is the most convenient and securest scheme, considering factors such as the personal expertise and network, location, and the market practices in the relevant jurisdictions.\textsuperscript{75}

### 3.3.6 How Does This Translate to Compliance Work of Obliged Entities?

In their CDD work, obliged entities should strive to identify the beneficial owners. This exercise is likely to get facilitated by the introduction of national beneficial ownership registers. This is an instrument introduced by the AMLD with the purpose of increasing the transparency and accessibility of beneficial ownership information. Enhanced CDD certainly has to be applied where the obliged entity finds discrepancies between the registry information and information collected by itself.\textsuperscript{76}

In the gambling industry, the customer base consists predominantly of \textit{natural persons}. Where the customer is a legal person and features in addition an unusual or complex structure, the gambling operator will regularly have to consider this a higher risk situation and apply enhanced CDD measures. Where B2B partners are legal persons, there is obviously nothing unusual about it; this is the normal case.

Accordingly, a complex company structure does not seem problematic as such. Where B2B partners or customers evidence transparent behaviour towards their gambling operators, making it easy for the latter to identify the beneficial owners (including dormant partners) and where needed verify that information, the situation can be acceptable, notably if it is accompanied by an effective continued monitoring.

By contrast, where representatives of such company structures seem unwilling to provide verifiable information, provide inaccurate or misleading information or are otherwise intransparent the gambling operator finds itself in a higher risk scenario that requires further CDD measures. Identifying the senior manager as beneficial owner\textsuperscript{77} is only a last resort when no other beneficial owner can be identified after a documented in-depth assessment (e.g. split shareholdings).\textsuperscript{78} This

\textsuperscript{72} European Commission (2017) SNRA, p. 9.
\textsuperscript{73} Irwin, Choo and Liu (2012), p. 105. According to these authors, however, terrorism financers by contrast would prefer using just a few techniques that allow for high levels of anonymity and appear innocuous.
\textsuperscript{74} Simser J (2013) Money laundering: Emerging threats and trends.
\textsuperscript{75} European Commission (2017) SNRA, p. 9.
\textsuperscript{76} European Commission (2017) SNRA, p. 17.
\textsuperscript{77} In view of identifying beneficial ownership in situations of split shareholding, the 3rd AMLD suggested a 25% share ownership threshold for defining a controlling element. European Commission (2017) SNRA, p. 9.
\textsuperscript{78} European Commission (2017) SNRA, p. 9.
should be duly highlighted in the record keeping, namely in the customer profile. In such constellation, an obliged entity is well advised not to on-board that client or at the very least to deal with the situation by increased monitoring efforts.

As an expert rightly noted taking a close look at the initial funding (and payment flows) of the early structures may bring more clarity than simply looking at abstract structures. Moreover, if the inquiry reveals a PEP within the company structure or initial funding, this increases the risk scenario – all the more if during the KYC communication with that company the PEP aspect was not disclosed or somebody else indicated as the beneficial owner (instead of the PEP).

Gambling providers are further well advised to consider not only persons who currently hold prominent public functions but also those who have done so in the past. A reading of various language versions of the AMLD clearly suggests this interpretation. Yet, the PEP risk factor is likely to fade out over time. It may be difficult for instance for a judge who retired 10 years ago to exercise illegitimate influence on court decisions (cf. corruption). It would thus seem unreasonable and disproportionate to apply to such person the same CDD standards as to an active high court judge.

Some laws give indications as per the relevant time frame. Liechtenstein law includes persons in the definition of PEPs who have exercised the high public office until a year ago. In line with the RBA the FMA Guidance suggests that the obliged entity must assess on a case-by-case basis whether an increased risk was still present. Risks do not take a sudden end upon retirement from the public position. Therefore, it may well be that an obliged entity concludes that a risk is still present and that enhanced CDD measures apply in spite of the cool down phase of 1 year having expired. On the other hand, if the PEP is no longer categorised as ‘higher risk’, his / her family members and close associates should enjoy the same down listing, too.

### 3.3.7 Complex, Unusual and Unusually Large Transactions

"18(2) Member States shall require obliged entities to examine, as far as reasonably possible, the background and purpose of all complex and unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. In particular, obliged entities shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious."

The present provision is not included in the annexes of the AMLD contrary to the other risk factors. The passage is part of Article 18 in the main text, refers to transactions and is addressed to the member states of the EU. The provision is nevertheless included here as it refers to three elements that we have already dealt with in section 3.3: “complex”, “unusual” and “no economic purpose”.

---

80 Art. 3(9): ‘politically exposed person’ means a natural person who is or who has been entrusted with prominent public functions; German: die wichtige öffentliche Ämter ausübt oder ausgeübt hat; French: qui occupe ou s'est vue confier; Italian: che ricopre o ha ricoperto.
81 Art. 2(1) lit. h Due Diligence Act.
82 FMA Guidance 2013/1, p. 3.
3.3.7.1 Online Gambling Regulators

One regulator responded that he would hope that this was standard AML practice and that regulators would apply this towards their operators. Another regulator argued that this provision was to be interpreted by national legislation. Finally, yet another regulator argued that this provision was more appropriate for financial services businesses. In the online gambling business, this provision could refer for instance to any unusually large wager or series of wagers, which would then require enhanced CDD and monitoring efforts.

3.3.7.2 No Apparent Economic or Lawful Purpose

It is noteworthy that Article 18 uses as an overall condition the term “which have no apparent economic or lawful purpose”. In my view, this condition applies both to “complex and unusually large” as well as to “unusual patterns”. We had already noted that the absence of an economic purpose was a good indicator for a higher risk constellation.

The provision further mentions “no lawful” purpose. To illustrate a lawful purpose: it may be difficult or simply impossible to receive for instance an authorisation for a certain business in some jurisdictions (e.g., prohibition or monopolisation of a business), while it is possible to seek establishment and a license in other jurisdictions. Accordingly, there may be legitimate reasons for setting up a business in foreign jurisdictions. These regulatory elements are likely to be considered for instance by a bank (i.e., an obliged entity) that receives payments from gambling providers on customer accounts of that bank.

One expert welcomed the fact that the obliged entities were expected under Article 18 to properly understand what they are facilitating through their services. The obliged entity had to ask questions and insist in getting sound answers. Another expert noted that this provision was essentially taken over from FATF and could address for instance a situation where a public employee receives EUR 50’000 on his account without any plausible reason being recognisable for the bank.

3.3.7.3 What Is a Complex, Unusual or Unusually Large Transaction?

The Liechtenstein FMA describes the nature of complex transactions in their guidelines and underlines that the assessment always needed to be done on a case-by-case basis. The legal provision was aimed primarily at transactions where the complexity of the transaction hindered the transparency in relation to information that is relevant for CDD work. The authority mentions as examples derivatives traded outside stock exchange or a transaction executed through complex structures or by involving several jurisdictions. Indeed, illicit funds can easily be split up within a complex labyrinth of financial transactions that are all in support of the layering process.

---

83 FMA Guidance 2013/1, p. 7.
Finally, in relation to unusual transactions, the Guernsey guidelines refer to the earlier mentioned comparison between expected pattern of transaction and actually monitored pattern of transaction. We have seen the relevance of this inconsistency in the context of the customer profile. The guidelines describe inconsistency in relation to the activity within a particular business relationship or with the normal business activities for the type of product or service that is being delivered. If there was no apparent economic or lawful purpose visible, this could indicate money laundering.\textsuperscript{85}

3.4 "Products or Transactions that Might Favour Anonymity"

3.4.1 Gambling Regulators

It should be noted from the outset that this risk factor (“might favour anonymity”) is not equivalent to the risk factor that we shall subsequently examine (“non-face-to-face business relationships or transactions”). It became clear from the responses of the gambling regulators that they as well see clear differences between the two constellations. This is particularly noteworthy as some reports and authors keep confusing the two constellations: “Given that online gambling, by its nature, is conducted anonymously, the use of false or stolen identities is less likely to be detected.”

According to the gambling regulators there is no room for anonymity in the gambling sector. Anonymity was anathema to AML policies. The customer had to be identified and anonymous transactions avoided. If the laws of a jurisdiction allowed anonymous players for anything above trivial stakes and/or prizes, criminals would try to exploit it.

One regulator argued that some products might not allow the operator to adequately identify the customer and/or track their transactions (e.g., wins and losses) or where the beneficial ownership was unknown. They saw examples in multiple platforms such as online poker and transactions that involved cash or anonymous payment methods such as prepaid cards.

3.4.2 The Old Days of Banking

According to some experts, anonymity was possible in the old days of banking. An expression of anonymity were the numbered accounts, an arrangement in which the name of the account holder was kept secret and banking staff were unable to look up the identity of the account holder in the bank registry. The account holder instead identified himself by means of a code word. And only a very limited number of bank employees would have access even to that code word. One expert anecdotally noted that some fictitious names used to be particularly popular as code words such as ‘James Bond’ or variations thereof.

While numbered accounts still exist, they have arguably lost their anonymity in most countries; customers can no longer open an account without the banking staff inquiring their identity. In fact, anonymity is hardly imaginable nowadays in a reputable financial market. If a compliance officer cannot find the identify of an account holder in the bank’s data system or if he was denied access to that information, this would have to trigger a red flag.

---

86 MONEYVAL (2013) The use of online gambling for money laundering and the financing of terrorism purposes, p. 15.
87 In the past, international banks had to pay high fines for the violation of regulatory requirements (other than AML); this arguably has raised awareness of regulatory requirements and reputational risk. Schooner HM, Taylor MW (2010) Global bank regulation: Principles and policies. For a regulatory discussion in the US context see Guynn RD (2014) Regulation of foreign banks and affiliates in the United States.
3.4.3 Delimitations and De Minimis Rules

We had noted that anonymity must be first of all distinguished from non-face-to-face situations. Furthermore, illegitimate motives driving anonymity must be distinguished from the legitimate motive of discretion that we dealt with earlier. Discretion does not need to hinder effect AML compliance work. At the same time, discretion cannot serve as justification for anonymity. Accordingly, identification and verification must be properly done where required by law. As part of appropriate KYC work, obliged entities must insist that scans of ID documents are of sufficient quality. Where they have failed in doing so, regulatory authorities have imposed severe sanctions.\(^{88}\)

One expert further argued that gambling with low stakes and low pay-outs could be treated differently thereby suggesting a de minimis approach (i.e., thresholds under which normal CDD would not be required). Indeed, the AMLD defines lower risk scenarios in relation to small transactions, as we shall see later on.

It was suggested that debit cards linked to bank accounts that are covered by strict bank secrecy laws helped to keep transactions concealed.\(^ {89}\) Yet, anonymity must nevertheless be distinguished from bank secrecy. The fact that a jurisdiction practices a policy of secrecy regarding the bank customer does not mean that the customer enjoys anonymity towards the bank or the prosecutors in case of criminal investigations. In any event, with the adoption of the Automated Information Exchange (AIE) the bank secrecy has largely lost its meaning at least in the international sphere.

3.4.4 Cash and Other Anonymous Products

While there are sector-specific vulnerabilities, there are also some that are of cross-sectorial nature. One cross-sectorial vulnerability is anonymity in financial transactions, i.e., the use of cash or other anonymous financial products.

Organised crime tries to avoid paper trail or any other information linking them to illegal activities. Without specific KYC policies in place, cash transactions allow for complete anonymity, making them a very attractive payment method for money launderers. This circumstance puts business sectors at particular risk that are exposed to high levels of cash transactions.\(^ {90}\) This is notably the case for traders in goods and services accepting high payments in cash as well as and economic operators accepting payments in large value denominations, such as EUR 500 and EUR 200 banknotes.\(^ {91}\)

We had already noted that cash may make its way into online gambling through mixed gambling chains, that is, where online operators’ websites are cooperating or even run by a land-based casino.

---

\(^{88}\) Cf. for instance the Plus500 case where the Financial Conduct Authority (FCA) ordered Plus500 in 2015 to freeze thousands of customer accounts while inquiring the company’s AML practices.

\(^{89}\) Nixon, Bedi and Kamolchanokkul (2004).


Similarly higher risks apply to certain goods that are easily tradable and transferable and can be safely stored. These goods include for instance gold, which is popular due to its universally accepted value. Gold can provide anonymity and its shape can rather easily be changed, too. More innovative techniques include double invoicing, false shipments, and other fraudulent practices. Precious stones (e.g., diamonds), art objects and antiques (e.g., rare stamps) are attractive, too. Fraudulent practices include the provisioning of false certificates of sale or phony reproductions of masterpieces. These objects too can be moved from one country to another and sold internationally at market value to integrate the funds.

Automated teller machines (ATMs) are yet another cash channel that has shown exposure to money laundering. Higher risks exist where ATMs are not bank-owned but run by separate independent businesses. Yet, the ATMs only form one aspect in more complex and sophisticated money laundering schemes. Bankcards issued by financial institutes in jurisdictions with weak AML policies make it easier to hide ATM transactions as they leave only minimal trail of financial breadcrumbs that could be followed.

3.4.5 Traditional vs Alternative Payment Methods

The literature often distinguishes between traditional and alternative payment methods. While the line between the two is not always clear, debit and credit cards, cheques and wire transfers are often referred to as traditional payment methods.

By contrast, online payment providers, prepaid cards and e-cash are seen as alternative payment methods. They can offer anonymity features similar to those of cash and place an intrinsic limitation on identification and monitoring possibilities. However, the Commission sees the respective risk levels nevertheless somehow lower since these products require more sophisticated planning, cover lower volumes of transactions and may be subject to a certain level of monitoring.

The Commission identified essentially two vulnerabilities in relation to alternative payment methods: first, the use of online financial intermediaries that are not subject to adequate AML regulation to deposit funds on gambling accounts, second, the use of prepaid cards that are

---

subject to lighter CDD requirements.\textsuperscript{97} One way of mitigating payment risks is to allow for online gambling only where funds are transferred through regulated financial service providers.\textsuperscript{98}

Prepaid cards can come with anonymity, no credit checks, worldwide acceptance, and the convenience of easy access, including in non-financial institutions such as retailers. Using cash to fund a pre-paid card poses similar risks as cash. And according to the FAFT report, casinos cannot make the same level of cross reference checks on some types of pre-paid cards as they are able to perform on financial institution accounts.\textsuperscript{99}

Not all e-wallets are licensed in reputable jurisdictions and some may accept cash as deposits. Other e-wallets may only accept transfers from financial institution accounts in the customer's name; yet, the statements issued by the financial institution may only record the payment to the e-wallet but not the transaction to the online gambling provider. This would seem convenient for money launderers who wish to disguise their gambling.\textsuperscript{100}

\section*{3.4.6 FinTech, Crowdfunding and Bitcoin – Becoming Part of the AMLD Framework?}

FinTech aims to introduce new technological solutions for speedier, secure and more efficient financial products. The Commission sees additional risks in the on-going growth of FinTech\textsuperscript{101} and in order to adapt to on-going technological developments, further analysis will be required to understand these risks.

The use of online payment services is expected to further increase in the digital economy. The related identity risks will also further boost the demand for reliable KYC tools in identifying customers. Accordingly, the Commission recommended that member states should ensure that the exemption thresholds granted to electronic money products are as low as possible to avoid their misuse.\textsuperscript{102}

These emerging products include crowdfunding platforms and virtual currencies. An expert noted that crypto-currencies such as bitcoin were not necessarily anonymous. But they nevertheless pose certain questions as regards money-laundering risks.\textsuperscript{103} Crypto-currencies come increasingly on the regulatory radar of the supervisory authorities.\textsuperscript{104}

\begin{thebibliography}{99}
\bibitem{98} MONEYVAL (2013) The use of online gambling for money laundering and the financing of terrorism purposes, p. 16 i.i.
\bibitem{100} FATF (2008) RBA Guidance for Casinos, p. 28: See below regarding the related issue of casinos purposefully obscuring payments made to financial institution accounts held by customers.
\bibitem{101} European Commission (2017) SNRA, p. 18.
\bibitem{102} European Commission (2017) SNRA, p. 18.
\end{thebibliography}
Moreover, crypto-currencies are not yet covered by the EU’s AML legal framework. Member States, however, can of course already extend the scope of the AMLD to professionals particularly at risk and can consider including crowdfunding, virtual currency platforms and e-wallet providers.

The Commission in fact has proposed to amend the AMLD and bring virtual currencies exchange platforms and wallet providers within the scope of the directive in order to further reduce anonymity in transactions. And the possibilities for electronic money products to be exempted from AML requirements will be further restricted. The Commission has further set up an internal FinTech task force to assess technological developments, technology-enabled services and business models. The task force’s work will notably relate to crowdfunding and crypto-currencies.

---

106 European Commission (2017) SNRA, p. 18. In this context, other vulnerable sectors are mentioned, too, such as auction houses, art and antiques dealers and specific traders in high-value goods.
3.5 "Non-Face-to-Face Business Relationships or Transactions, without Certain Safeguards, such as Electronic Signatures”

3.5.1 Online Gambling Regulators

The wording of this provision seems to suggest that online gambling per se and payments relating hereto represented a higher risk situation. The gambling regulators did not agree with this critical view expressed towards non-face-to-face relationships. Even where one regulator noted that non-face-to-face relationships could carry a theoretically higher risk, he argued that adequate identity checks could easily mitigate the risk.

One regulator most clearly rejected this risk factor noting that the theoretical security yielded by face-to-face business was simply meaningless in a mass-market environment. A transaction conducted in a land-based casino was no more money laundering-proof than one conducted over the Internet. To illustrate: Casino patrons would not talk to the casino managers every time they arrived at the venue or for each transaction they make.

Finally, one regulator pointed at a relationship that is often neglected in the AML discussion. He noted that the take-on process for B2B partners should be more rigorous and establish corporate structure, diligence on the controllers, source of wealth, etc., i.e., applying those measures that usually deter illegitimate businesses from trying to enter the space.

3.5.2 Internet Leading to Higher Risk?

The way the risk factor is described, it seems to suggest: a face-to-face relationship is safe, a non-face-to-face relationship means higher risk. Accordingly, online gambling services as a whole would involve nothing but higher risk circumstances. After all, the interaction between operator and customer takes place almost exclusively in non-face-to-face situations. The somehow simplified theory goes that Internet operators do not know their customers because they do not meet them and are unable to form social relationships with them. By contrast, land-based casinos know their customers because they meet them.109

The regulators did not agree with this view. Nor did the experts. In fact, it would seem that such binary view turns out to be a red herring. It can be misleading for AML compliance work to perceive face-to-face situations as safe or safer while perceiving remote situations as riskier. Believing in the ‘safety’ of face-to-face situations can lead to a deceiving sense of comfort and lax, negligent CDD practices. In land-based gambling settings, somebody can also show up with a fake ID (somebody else’s identity or made up identity) and get away with it, all the more in situations of mass market.

One expert added that this risk factor was further misleading in that it solely promoted to follow the individual, whereas following the money was often the more effective AML policy.

Defendants of this risk factor may argue that it does not portray all non-face-to-face relationships and transactions as higher risk but only those without certain safeguards. In my view, the argument is invalid as can be shown by applying the argument to land-based situations: Face-to-face situations “without certain safeguards, such as...” seem riskier as well.

3.5.3 Internet Providing Additional Technical Possibilities

Identity theft and fraud are legitimate concerns in relation to remote businesses. Profile details of player accounts, including payment details can be stolen and misused for non-approved payments. Stolen identities may further be used to open accounts with other service providers. Non-face-to-face business relationships or transactions can thus carry risks.

Yet, the Internet also provides for alternative or additional technical tools that can be used for AML compliance work. Notably, the Internet offers theft and fraud prevention measures that are not easily available in the land-based sphere. Such measures can rely upon new technologies, including the deposit and withdrawal methods offered on the website, and checks on the customers' Internet provider (IP) address.\textsuperscript{110}

IP checks are useful in preventing criminals for instance from opening multiple casino accounts by using stolen identities. Internet casinos have a strong interest in providing adequate data security to their customers and thereby avoiding that their data gets stolen.\textsuperscript{111} Furthermore, the information provided by the customer can instantly be double-checked by a range of positive and negative checks.

Obliged entities can use checks that go beyond basic database checks and traditional checks using customer's personal and official documents. They could demand information on and look into customers' sources of funds and get in direct contact with the customers via telephone or video conferencing.\textsuperscript{112}

3.5.4 Why Was Non-Face-to-Face Included?

If there is such broad criticism towards this risk factor, one must unavoidably ask the question why it was included in the first place.

One expert explained the inclusion with historical reasons. In the past, non-face-to-face was seen as almost equivalent to anonymous; similar non-face-to-face critical wording can be found in FATF documents. What is more, AML compliance was traditionally steered towards and dominated by a perspective on the financial sector. And the usual customer setting in a bank was to meet him face-to-face at the bank counter (or alternatively in more discreet and luxurious bank facilities). Anything deviating from this setting was seen as unusual and thus higher risk. This is supported by a

\textsuperscript{111} FATF (2008) RBA Guidance for Casinos, p. 28.  
statement of another expert according to whom financial institutions were in some countries even nowadays not allowed to do business without in person meetings.

There is a further reason that in my view applies. It regards a classic phenomenon of law making: it is always harder to eliminate a provision (or an assumption that is behind a legal provision) than to simply keep it in the law. And after all, these concerns and assumptions were not invented by the European Commission but taken over from similar wording in FATF. It is a human trait to tend towards inertia, which is a well-described phenomenon in behavioural sciences. As if the paradigm was: if we want to eliminate it, we will have to argue this thoroughly; if we want to keep it in – well, we have already provided the reasons in the past.

3.5.5 Threat for Innovation: FinTech and the Relevance for the Online Gambling Industry

Taken together, the risk factors ‘non-face-to-face’ and ‘new products and new business practices’ (to be dealt with in the next section) express a rather conservative and critical view on innovation. New technologies usually come with challenges and opportunities. But rather than seeing the opportunities that new technology will offer, the potential risks are emphasised. The inclusion of the vaguely phrased risk factors in the AMLD per se is not a big issue for technological innovation but it can become a substantial problem when national authorities adopt regulation that takes such critical view (i.e., legislator, regulators und supervisors) and implement detailed restrictions that hinder technological innovation.

Innovation-critical policies hold the tangible potential to become a heavy burden on innovation-driven sectors. In the context of online gambling, FinTech should be mentioned. FinTech describes a fast-growing business sector that works on new technologies in the area of financial services. FinTech firms and their new solutions compete with the more traditional financial methods. FinTech makes financial services easier and more accessible. An example includes the use of FinTech apps on smartphones to enable mobile banking.

High levels of mobile penetration and FinTech apps have revolutionised online gambling, which moves more and more away from stationary computers to mobile devices. If an online operator wishes to have an attractive mobile gambling offer, it simply has to adopt smoothly and fast working mobile payment solutions. Customer experience is key for gambling operators who want sustainable success among players. As a consequence, burdensome restrictions on FinTech also have effects on the sectors applying these solutions, including the online gambling industry. Another possible outcome can be that the latter is not able for regulatory reasons to introduce recent FinTech solutions in spite of them being available.

It goes without saying that innovation-friendly and -driven economies will see such scenario as threatening. A couple of experts confirmed that especially smaller and dynamic countries would see this as problematic.

3.5.6 Technology Applied to Non-Face-to-Face

We had noted that the overly sceptic view on online business relationships seemed no longer justified given new technological circumstances. The FATF noted that in remote situations, obliged entities were unable to verify customer’s physical appearance against photographic identification documents.\(^{115}\) This generic statement seems exaggerated if not inaccurate. Online / video instruments offer sufficient possibilities to check the physical appearance and the photo ID as we shall see below.

Where national regulators enjoy the necessary discretionary powers, i.e. where national law does not hinder technological solutions, they can take steps to promote technology- and innovation-friendly practices. FINMA for instance has taken the position that “video identification has equal validity to in-person identification”\(^{116}\) if obliged entities respect certain technical and organisational requirements:

- Identification to be made via audio-visual real-time communication between contracting party and obliged entity
- Obliged entity ensures through adequate technical equipment the secure video transmission as well as the reading and decryption of the information stored in the identification document’s machine-readable zone (MRZ)
- Picture and sound quality adequate to enable unambiguous identification
- Obliged entity can use technical aids to compensate for poor lighting (especially when taking photographs required for identification)
- Specially trained employees of the obliged entity responsible for identifying the contracting party
- Full duration of interview to be audio-recorded
- Obliged entity to define a process for conducting the identification interview and a dialogue guide for the employees responsible for video identification.

Prior to the call, the contracting party provides the required details electronically. During the identification interview, the obliged entity checks the information and is expected to look for conspicuous behavioural patterns that could indicate the non-authenticity of the identification documents. Further, the obliged entity takes photographs of the contracting party and the identification documents.

Authenticity of the identification documents is further reviewed by the use of a machine that reads and decrypts the information in the MRZ and by examining some of the optically variable features (e.g., the kinegram by tilting the ID). As an additional identification tool, a transaction authentication

number (TAN) can be used: this is a single use one-time password as commonly used in online banking. All this is to be comprehensively documented, filed and archived.

Under the same conditions, video identification can be performed for more than one contracting parties as well as in relation to legal entities or partnerships. Under certain conditions, the obliged entity can mandate third parties with the identification / verification process. As an alternative to the video identification, the obliged entity may also choose online identification for which detailed guidance is offered, too.

Similar conditions have been outlined by the Liechtenstein FMA for online / video identification. The legal effect of this non-face-to-face protocol is that the on-boarding (of the customer) can be regarded as if it had been performed “in-person”. As a consequence, enhanced CDD will generally not be triggered in such cases.

117 FINMA (2016) Circular 2016/7 Video and Online Identification, pts 23-27. Additionally, an extract from a directory and a copy of the power of attorney is required.
119 FINMA (2016) Circular 2016/7 Video and Online Identification, pts 29-44.
3.6 "New Products and New Business Practices, Including New Delivery Mechanism, and the Use of New or Developing Technologies for Both New and Pre-Existing Products"

3.6.1 Online Gambling Regulators

The replies of the regulators regarding this risk factor were somehow more divergent than in relation to the earlier factors.

One regulator interpreted the notion as any new product or business practice where controls to mitigate the money laundering risks were not yet fully understood or developed. He mentioned the example of ‘blockchain’ technology and virtual currencies. But also new ways in which the product is delivered to the customer such as changes in the delivery platform (mobile, TV, social media, etc.) or even totally new or unique gambling products.

Another regulator found this risk factor sound, noting that new products and business practices required careful management to make sure that they did not represent an opportunity for criminal exploitation.

Finally, another regulator argued that this was not how a regulator would typically approach due diligence. The relevant regulatory topics – no matter new products / business practices or not – would typically regard ownership, source of wealth, credentials, etc.

3.6.2 Are New Products Automatically Higher Risk?\(^{121}\)

Several experts joined the critical view on this risk factor expressed by the aforementioned regulator (“this is not how to approach due diligence”). This reminds of the comments on the earlier risk factor “non-face-to-face”. Some experts had noted that this provision made innovation look suspicious and could lead to technology-averse policies. It was an example of a traditionalist conservative approach stemming in Europe typically from bigger member states. Smaller countries by contrast were often more agile in introducing new technologies.

This criticism seems sound. The way the risk factor is phrased is too absolute and can result in killing innovation if strictly implemented by national authorities (cf. earlier). It seems that one simple addition to the wording of the provision would make things less innovation-critical and more focused on the actual issue: “New products and new business practices can only be seen as higher risk when they feature new risks and controls to mitigate the money laundering risks are not yet understood or developed.”

\(^{121}\) Some aspects that could be dealt with under this section have already been dealt with in earlier sections (e.g., “anonymous”; “non-face-to-face”) where they fit, too (e.g., crypto-currencies). There are not dealt with in this section to avoid redundancy.
The rephrased wording does not portray innovation and progress as dangerous or more risky. Innovation is welcome. The risk is present when innovative products and new practices are implemented without asking: First, does this bring new money laundering risks? How could criminals use this product / practice for their purposes? And second, if there are new risks, how can we mitigate them? Are these mitigating solutions available? If the mitigating measures are not yet developed and the risks are clearly more than theoretical, the obliged entity is arguably well advised to apply enhanced CDD to such new product or business practice.

Similar to the views expressed by some regulators and experts, this suggested approach does not see each new product (innovation) per se as higher risk. Many products may in fact not bring any increase in AML risks. However, where obliged entities do not ask themselves the aforementioned suggested questions and act accordingly, this may very well lead to higher risk situations. This adjusted approach seems somehow more aligned with what can also be found in the FATF recommendations:

“Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.”

The notion “identify and assess risks” refers to the due diligence questions that I suggested in this section. In other words: FATF did not share the view that new products automatically lead to higher risk situations. It is further noteworthy that FATF recognised an obligation to identify and assess risks only in relation to “countries and financial institutions”. Yet, this wording is due to FATF’s particular focus on the financial sector that can be noticed throughout its recommendations.

---

122 FATF recommendations (2012), pt 15.
3.7 “Financial Products or Services that Provide Appropriately Defined and Limited Services to Certain Types of Customers, so as to Increase Access for Financial Inclusion Purposes”

Apart from “higher risk” situations in Annex II the AMLD further describes “lower risk” situations in Annex III. Among the latter, two notions appear as broad and indistinct. Since they represent, however, “lower risk” in the Commission’s view they are not as extensively discussed as some of the earlier notions.

3.7.1 Online Gambling Regulators

Two gambling operators concurred that this lower risk factor had no relevance in the i-gambling sector.

One regulator recognised the value of “financial inclusion” and that it was a great ally in the fight against money laundering. Accordingly, this factor could apply to certain low risk gambling products.

But the regulator further noted that regulators should also have an eye on the financial means of the players. Financially excluded persons tended to be those with lower incomes. Accordingly, the financially inclusive gambling products would need to be controlled so that people with limited means - often gambling in the hope of no longer being constrained by limited means - did not spend money that they could ill afford to lose on gambling.

3.7.2 Defining Lower Risk?

While the AMLD has chosen to define certain lower risk scenarios, this is not necessarily the case in national AML laws. Swiss law for instance does not define lower risk scenarios but only higher risk scenarios. Similarly, as far as can be seen, the US do not define lower risk scenarios either.

The conversations with experts showed that some questioned the appropriateness of defining lower risk scenarios. Their rationale is that the legislator should not cause obliged entities to become less cautious in their risk assessment. It was for them to do the risk assessment.

Indeed, the question may be asked what the motivation would be for a legislator to expressly define low risk scenarios. To fully recognise the rationale for this lower risk factor, one has to move away from a mere AML perspective and take other legitimate policy goals into account, too. “Financial inclusion” is an agenda that is not only pursued by the EU but also by the FATF and some of its member states. It is also a response to unintended side effects of AML requirements formerly applied.
3.7.3 What Is Financial Inclusion?

In answering this question, one must address the issue of unintended consequences of AML rules. One expert gave an illustrative example of a financial inclusion measure. In South Africa (as in other countries), AML policies required that everybody intending to open or keep a bank account had to declare his address. However, this requirement turned out to be impracticable in reality. Since some customers lived in townships they were not able to indicate a precise address – and as a consequence found themselves in a situation of “financial exclusion”.

In response to this issue, it was agreed that this customer segment should be regarded as lower risk with simplified CDD requirements applying. The de-risking in this concrete example was necessary since rejected bank customers would otherwise have been pushed into other payment solutions, including potentially illegal ones (not duly registered and regulated). Ultimately, this is a balancing exercising involving different policy goals.123

3.7.4 Relevance for Online Gambling Sector?

Concurring with two regulators the direct relevance of this notion for online gambling seems very limited; this is also what the responses from the experts suggested. According to some of them, the notion “certain types of customers” could for instance mean a purely national customer base or the fact of extending the scope of services to a pre-existing, pre-defined customer group, which was already thoroughly checked or finally, the description could apply to non-commercial institutions providing certain services. The vagueness in the responses confirms that little direct application was recognisable.

3.7.5 The Example of Hawala

The aforementioned example from South African illustrates how certain segments of customers may get excluded from financial channels. The goal of financial inclusion agendas accordingly is to bring people back to the official financial channels. As a regulator noted, financial inclusion can work as an effective ally in the fight against money laundering. This is correct. The strictest AML provisions on official financial channels are of little use when a good part of the economy simply avoids these channels or is pushed out of them, opting instead for unofficial channels that are not subject of AML checks.

Hawala is a good example of unofficial channels, an informal payment system traditionally popular in the Orient. The Hawala financial system allows for international transfers of money or other goods (money worth). Payments can be transferred fast and at low costs. The following example shall illustrate Hawala:

A in Germany owes EUR 10’000 to B in Turkey. Normally, he could make an online wire transfer from his German bank to B’s bank in Turkey. In Hawala, A gives the EUR 10’000 in cash to Y who also resides in Germany. Y contacts his Hawala colleague Z in Turkey asking him to pay the equivalent of EUR 10’000 in Turkish currency to B. In the beginning, A had defined a code word, which was independently communicated to B as well as Z (through Y). Since B is able to state the correct code word towards Z, the latter pays out the money to B.

The Hawala system at first sight reminds of payment systems such as Western Union. Yet, at Western Union the financial institution acts both as Y and Z. Moreover, in the ideal case the transfer through Hawala only takes a few minutes. At the same time, Hawala is more complex: If Y does not pay Z for one transfer, Z will hold it against him in future transfers. Ultimately, the system relies on trust and trustworthiness. It further avoids incurring banking fees or any potentially applicable taxes.

Figure 3: Hawala

From an AML perspective it is important to note that the whole payment procedure through Hawala can largely be done anonymously. Normally, A and B do not need to identify themselves to Y and Z by their names but only by way of a code. What is more, they do not need to disclose the source of the money. It is therefore evident that that Hawala does not apply CDD regarding fundamental aspects of any effective AML policy.

It is therefore not surprising that the Commission pointed at this issue in its SNRA while also taking note of the fact that the size of the issue is hardly known. The Commission, however, emphasised mostly the risks in relation to terrorism financing. Payment service providers should normally be registered and regulated (cf. Art. 4(3) of Payment Services Directive 2). Hawala and similar services do not follow these requirements and it is hard to detect their existence:

---

transactions are bundled, compensated via goods imports/exports, and leave limited information trail.\textsuperscript{125}

FATF has recognised this problem, too. It provided guidance in relation to financial inclusion in its 2013 publication “Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion”.\textsuperscript{126}

\textsuperscript{125} European Commission (2017) SNRA, p. 15.

\textsuperscript{126} FATF (2013) Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion. The FATF guidance is currently under revision and an updated version is forthcoming.
3.8 "Products where the Risks of Money Laundering and Terrorist Financing are Managed by other Factors such as Purse Limits or Transparency of Ownership (e.g. Certain Types of Electronic Money)"

3.8.1 Online Gambling Regulators

One regulator found it reasonable to define these circumstances as lower risk. Another regulator, however, noted that the lower risk factors seemed to overlap national lottery models quite neatly. It could be anticipated, if this became recognised as lower risk, criminals would target it.

3.8.2 Prepaid Cards and E-Wallets

Products with purse limits in the gambling sector may include prepaid cards and e-wallets. They have already been dealt with in this report.\textsuperscript{127} As noted, the AML issue with these payment tools is anonymity. One may therefore wonder why they are listed among lower risk products in the AMLD. Indeed, some experts argued that they recommend defining only higher risk constellations but not lower risk.

The likely rationale for the inclusion of these products can be seen in the inefficiency for criminals. Money launderers will find efficient means more attractive than inefficient means. This obviously also includes the amount of money that can be laundered in one go. If member states (and/or obliged entities) define very low purse limits, criminals may not find it very efficient to launder money through these payment channels.

3.8.3 Transparency of Ownership

In relation to transparency of ownership, one expert mentioned stock-listed companies that have to comply with transparency requirements (e.g., when reaching a certain threshold of owning shares in a company, this must be made transparent). Another person mentioned scenarios where information relevant for customer due diligence work could be easily accessed.

The underlying rationale arguably is that transparent ownership makes money laundering unlikely. One may think in particular of either publically owned companies or large, internationally known companies that feature high credit ratings, sometimes referred to as Blue Chip companies. Yet, I agree with the aforementioned caveat of a regulator. The fame of a private company or the mere fact of a company being publically owned can very well serve as a red herring.

Where the attentiveness of AML staff is lowered due to this consideration, aspects that would be seen as suspicious in relation to other companies may get overlooked. Corporate scandals such as the one regarding Enron and Arthur Andersen LLP illustrated that fame does not necessarily go

\textsuperscript{127} Cf. section 3.4.5 – 3.4.6.
hand in hand with high compliance standards. Similarly, publically owned companies are not immune towards AML risks. Lowered attentiveness and laxness in the on-boarding of new management / staff may well lead to a risk of infiltration in such publically owned company.

128 The Enron scandal did not relate to money laundering but to falsification of balance sheets. Enron's accounting firm Arthur Anderson LLP, too, formerly one of the big five, collapsed in the aftermath of the scandal. Well-known rating firms had given high ratings until prior to Enron's insolvency.
4. Mitigating the Risks

4.1 Finding the Right Balance

There is an additional question that regulators may ask themselves. Now that the money laundering risks scenarios have become clear: How do we specify effective regulatory AML requirements without unnecessarily burdening our gambling industry?

Having appreciated the risks, regulators are normally interested in learning about the means to mitigate the risks. These means should certainly be effective in achieving the policy objectives. At the same time, if the chosen means prove to be too far-reaching the regulated industry will suffer from the heavy regulatory burden. It would thus appear that proportionate AML measures are those measures that find the right balance between effectiveness and unnecessary burden. Proportionality should show the way ahead. After all, the principle of proportionality forms part of the fundamental principles of many constitutional legal orders. Proportionate are means that do not exceed what is necessary to achieve the objectives.¹²⁹

4.2 The Internet: Threat or Mitigating Nature?

In its staff working document, the European Commission analysed the money laundering risks in various business sectors.¹³⁰ Within the gambling sector, the Commission distinguished between the products betting, bingo, casinos, gaming machines, lotteries, poker, and online gambling. It is noteworthy that the Commission did not find it necessary to further divide “online gambling”, contrary to the land-based sector. For the Commission, the risks appeared to be primarily linked to the nature of online transactions.¹³¹

Regulatory discussions regarding the Internet often over-emphasise the threats regarding remote channels and neglect the opportunities that technology can offer. The Commission’s view expresses both sides. On the one hand, it expressly recognised the risk mitigating nature of the online channels that permit to track all transactions.¹³² On the other hand, it identified the lack of face-to-face contact as a main threat (apart from the risk of infiltration or ownership by criminal elements). Nevertheless, the Commission admitted that the “anonymity” could be minimised by proper controls and verification measures as well as by the traceability and tracking of electronic transactions.¹³³

The ambiguous wording regarding the threats and safeguards of online channels seems to contrast with the predominant view expressed by gambling regulators and experts in this research. They had noted, to some extent, a technology-averse wording in some of the AMLD’s higher risk

¹²⁹ Cf. e.g., Article 5(4) Treaty on the European Union (TEU): “Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties.” Cf. further Protocol No 2 of the TEU on the Application of the Principles of Subsidiarity and Proportionality.


factors. What is more, they had also criticised that two different things - “non-face-to-face” and “anonymous” - would often get confused. This also seemed to be the case in the Commission's assessment in relation to online gambling when it noted the “risks associated with the lack of face-to-face contact although the anonymity can be minimised” by controls and verification.

4.3 Mitigating Risks: By Way of Regulation?

Regulators may wonder whether and to which extent they should pass additional gambling sector-specific AML regulation. The answer is not straightforward and depends on the national setting. This shall be briefly illustrated below.

If a gambling regulator is located in a jurisdiction that features very robust AML legislation as well as a strong FIU (or similar authority), there may not be much need for extra gambling-specific AML regulation. Additionally, the FIU (or for instance the financial market supervisory authority) might have passed AML ordinances and / or guidelines that flesh out the expected conduct from obliged entities. And these requirements apply, directly or indirectly, to gambling companies, too. Additionally, the AML practice is backed up by committed law enforcement agencies. In such constellation, there may not be much need for additional regulation. Appropriate “soft measures” would seem to suffice (i.e., training, etc., cf below). Yet, the importance of a thorough fit & proper test in the course of the licensing procedure should not be underestimated. It can serve as an effective AML gatekeeper at the very early stage.

If, by contrast, another regulator is located in a jurisdiction that features weak AML legislation - for instance, since the national legislation ignores key AML requirements of the AMLD (or FATF) - as well as an understaffed or little qualified FIU (or similar authority), the regulator must ensure the integrity of his industry, pass appropriate regulation, and seek the necessary support for sufficient law enforcement in his industry. Clearly, in such constellation, it will be a significant weakness in terms of AML rules and enforcement if the gambling regulator does not dispose of enforcement powers (i.e., investigations, fines, etc.).

4.4 Mitigating Measures

The Commission suggested a series of mitigating measures separately for each product (e.g., lottery, poker, online gambling). Apart from minor differentiations, these measures are, however, similar throughout the portfolio of gambling products. Overall, these measures seem sound and appropriate. In the following, they are briefly summarised and commented on.

---

• **Improve cooperation between the relevant authorities: gambling regulator, FIU, law enforcement agencies**

In my view, the cooperation should most of all involve the exchange of expertise. Specialised AML professionals can help gambling regulators in understanding the risk factors, developing typologies as well as effective supervisory practices. While this measure would seem obvious and rather easy to implement, discussions with colleagues from various jurisdictions suggest that many regulators have thus far not used this opportunity.

• **Ensure regular cooperation between the relevant authorities and the online gambling operators**

A regular exchange, for example in the format of workshops, can provide helpful guidance to obliged entities, for instance in relation to gambling-specific AML risks and the quality of STR submissions. However, I would rather disagree with the suggestion that the increase of the number of STRs should constitute an aim in itself. The mere number of submissions does not say much about the size of the AML risks or the quality of the compliance work done by the obliged entity. STRs should be submitted when appropriate. An extreme interpretation of the duty to submit STRs can lead to the unwanted situation where an obliged entity simply outsources their compliance work to the FIU, resulting in a rapid increase of work load for the FIU. A logical consequence would be the call from the FIU for more staff and funding.

• **Training sessions of the staff and compliance officers**

This constitutes one of the best mitigating measure since it raises awareness among those who will have to detect suspicious transactions and circumstances in practice. The main contents of the training sessions could be defined jointly by the gambling regulator and the specialised national AML authority (e.g., the FIU) and the courses provided by (public or private) AML professionals. Continued education also means to raise the participants’ awareness of new and emerging risk factors such as e-money and virtual currencies.

• **Pooling resources with authorities from other jurisdictions**

Training sessions joined by staff from regulators and FIU’s of several jurisdictions can make a whole lot of sense particularly in relation to new or complex risk factors that are not yet well understood and in relation to which mitigating factors have hardly been applied.

---

• **Guidance on the safeguards in relation to online identification and verification**

Obliged entities may appreciate if the regulator (or FIU or other author) clearly defines the technical requirements, which their online identification and verification procedures have to comply with. This report has outlined some of the requirements that are already practised in European financial markets (e.g., FINMA guidelines in Switzerland).

• **FIUs should provide feedback**

One of the points that obliged entities within the gambling sector criticised in the workshops with the European Commission regarded the submission of STRs, more precisely, the follow up by the FIUs. Essentially, there was none, which is a problem for the obliged entities. Only if the FIUs engage in a continued dialogue can the obliged entities improve their reporting. Moreover, if the obliged entity is not duly informed about the status of the procedure, it may run into issues with the customer (e.g., withholding of money on player account, violation of data protection rules).\(^\text{138}\)

---

\(^{138}\) Obliged entities from other sectors may experience similar challenges: Stämpfli AA (2009) Kundendaten von Banken und Finanzdienstleistern.
5. Conclusion

At the beginning of this research stood the challenges that gambling regulators face in applying the AMLD requirements to their industry. Many other regulatory authorities, far beyond Europe and gambling, face very similar challenges: They too must interpret and apply broad and indistinct AML notions.

The drafters of such notions include the United Nations, the FATF, the EU, the Egmont Group, national legislators, financial market supervisory authorities, FIUs, and further bodies. They have defined AML requirements and i.a. circumstances in which higher money laundering risks prevail. Higher risks are for instance present when “the business relationship is conducted in unusual circumstances.”

Yet, what is this supposed to mean in practice? How is this notion to be interpreted by regulators in their supervisory and regulatory work? And how by the industry in their daily compliance work? It is my hope that this report has clarified some of these questions and provided helpful interpretive guidance to regulators and industry professionals alike.

Due to the very nature of the nine notions, simple definitions were not available nor were bullet point style descriptions appropriate. Each notion had to be thoroughly investigated and its characteristic aspects described. This research was strenuous not least because it involved detailed and technical AML specifications and language. Accordingly, one of the challenges was to compose the present guidance in appropriate language, that is, language, which is also approachable for regulatory authorities that may not be very familiar with AML matters. I hope that the report has found the right tone.

Summarising all notions in the conclusions or an executive summary did not seem appropriate and would have likely resulted in a dull condensed read. Instead, I shall outline some takeaways from this research.

One additional research question was how regulators could specify effective regulatory AML requirements without unnecessarily burdening their gambling industry. In other words: proportionate mitigating measures. In this context, regulators may wonder whether they should pass gambling sector-specific AML regulation. I hold the view that the answer is not straightforward as it depends on the national legal framework, notably the powers of the authorities involved in AML regulation, supervision and enforcement.

What matters ultimately is that the integrity of the industry is ensured. This can be the case in a jurisdiction that features very robust AML legislation, a strong FIU (or similar authority), sufficient guidelines, dedicated AML law enforcement, and the circumstance that gambling companies fall within the scope of these requirements. Accordingly, there may not be a pressing need for additional gambling-specific AML regulation. Another important factor is to which extent the gambling regulator is endowed with enforcement powers. If, however, the situation is different to the afore-described, it may be indicated for the gambling regulator to pass gambling-specific AML regulation to ensure the integrity of the industry.

139 Annex III pt 1 (a) AMLD.
I would further suggest that measures relating to capacity development seem appropriate. This includes a continued exchange between all relevant authorities as well as the industry. Regulators will better grasp the real AML issues when receiving support from FIUs and other bodies that feature substantial AML expertise. In turn, FIUs too can further develop their own capacity when deepening their understanding of gambling-specific circumstances. These are low hanging fruits that public authorities should pick.

Capacity development in the industry also means raising awareness among gambling companies’ staff and their compliance officers in particular. Increased awareness of money laundering typologies and AML requirements lowers chances that suspicious circumstances remain undetected. At the end of the day, what matters is that a credible AML culture is practised in the industry – arguably, this cannot be achieved simply by legislation and regulation. It takes top down leadership within each obliged entity.

It was not part of the research scope to assess the overall regulatory quality of the AMLD. The scope was focused on the interpretation of abstract AML notions. Some gambling regulators and experts (AML professionals) critically assessed certain wording of the AMLD. They noted a rather technology-averse tone in the AMLD. And some would undoubtedly give online gambling a lower threat and vulnerability rating than the Commission did.

In fairness, however, the European Commission’s big effort in preparing the AMLD and composing its supranational risk assessment (SNRA) must be recognised. Having attended some of the Commission’s workshops I was under the clear impression that the Commission invested significant time and effort during its SNRA to thoroughly analyse the threats and vulnerabilities of each sector, showing itself very open for input from industry professionals and AML experts.

When considering the various inputs for this research, it can be concluded that a good part of the initially searched literature was of rather limited use. There is no scarcity of AML literature, quite on the contrary. But much of it deals with classic AML themes and there is few empirically driven work. The major factor, however, was the circumstance that the scope of this report was fairly specific. And as a consequence, much of the more directly applicable literature originated from publications of AML-specialised bodies (e.g., reports and guidelines from FATF, FINMA, and FIUs).

The input stemming from the interviews with the AML professionals (experts) was generally speaking very relevant. Some provided valuable information on the genesis and political background of certain AML notions; the kind of information that is hard to find in publications. Finally, the input from gambling regulators was important to early on identify certain relevant themes and challenges. The significant AML expertise of these three (online) gambling regulators was clearly reflected in their responses.

My final note is on the value of discreetness. A virtue that is not to be confused with anonymity, I should emphasise in the context of AML research. The valuable input from gambling regulators

---


141 European Commission. SNRA, Annex 2, p. 180-182. The Commission rated the threat and vulnerability of online gambling at level 3 out of 4 (4 being the highest level).
and AML professionals became possible only because they were assured – and indeed they trusted – that their responses would be dealt with appropriate discreetness. If by contrast the present study had intended to quote the participants on specific statements, it would have been difficult for them to contribute in a meaningful way. This is particularly true in relation to officials since their words could be interpreted as official, binding statements of their respective authorities. In view of more research, this circumstance is noteworthy for other researchers, too. I therefore conclude by expressing my gratitude to the participants of this study.
6. Acknowledgments

I would like to thank the International Center for Gaming Regulation at the University of Nevada, Las Vegas (UNLV) for the generous support through its Fellowship Program. I thank Executive Director André Wilsenach and Associate Director Jennifer Roberts as well as the reviewers of my research submission for their helpful comments.

I further thank the following regulatory authorities, experts and European Commission staff members for their time and effort in contributing to this study. Their participation cannot be interpreted as necessarily sharing the views expressed in this report. Any errors are those of the author.

Finally, I would like to thank Ms Sarah Dietschweiler and Ms Sine Edal for their research assistance and Mr Lukas Vogt for technical support.

Gambling Authorities
Alderney Gambling Control Commission
Isle of Man Gambling Supervision Commission
UK Gambling Commission

Experts (AML professionals)
Ms Bianca Hennig Executive Officer, Legal / International Affairs, Financial Market Authority Liechtenstein, Vaduz
Ms Astghik Karamanukyan AML / CFT Monitoring and Training Unit at MONEYVAL (Council of Europe); Strasbourg
Ms Sören Meius Advisor at Ministry of Finance Estonia, formerly member of the Executive Board of Gaming Regulators European Forum (GREF) and Chairwoman of the Board of Eesti Loto, Tallinn
Dr Stiliano Ordolli Head of Money Laundering Reporting Office of Switzerland (MROS) at Federal Office of Police, Bern
Mr Michael Schöb Vice-Director of Financial Intelligence Unit (FIU) Liechtenstein, Vaduz
Mr Daniel Thelesklaf Director of Financial Intelligence Unit (FIU) Liechtenstein, Chair of MONEYVAL, Member of the Egmont Committee - Representative Europe II Region, Vaduz
Mr David Zollinger Attorney at law, formerly Swiss public prosecutor on AML matters, Wetzikon
<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ms Marianne Carrubba</td>
<td>Directorate-General Justice and Consumers, Financial Crime Unit, European Commission, Brussels</td>
</tr>
<tr>
<td>Mr David Schwander</td>
<td>Directorate-General Justice and Consumers, Financial Crime Unit, European Commission, Brussels</td>
</tr>
<tr>
<td>Mr Bertil Vagnhammar</td>
<td>Directorate-General Justice and Consumers, Financial Crime Unit, European Commission, Brussels</td>
</tr>
</tbody>
</table>
Bibliography

Books


von Feuerbach PJA (1801) Lehrbuch des gemeinen in Deutschland geltenden peinlichen Rechts. Heyer, Giessen.


**Book chapters**


Journal articles


**Other materials**

*Unless indicated differently, all materials last accessed on September 1st 2017.*


The aforementioned 4 documents relating to the SNRA can be accessed on: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272


FATF (no date) FATF members and observers. http://www.fatf-gafi.org/about/membersandobservers/.


