

Observations on the Gaming Industry: Business-2-Business Anti-money Laundering Risks and Trends



Foreword

According to the United Kingdom Gambling Commission (UKGC), licence holders should give due consideration to the money laundering risks posed by their business-to-business relationships, including any third parties they contract with. The assessment of these risks is based, among other things, on the risks posed to the operator by transactions with business associates and third-party suppliers such as payment providers, including their beneficial ownership structure and funding sources.

While customer due diligence receives most attention from gaming companies' legal and compliance departments, we believe business-to-business (B2B) relationship due diligence, which presents significant risk, is often overlooked

Over time we have seen many examples related to B2B relationships where gaming companies have conducted only a basic corporate verification check of a third party, focusing on their company number, country of incorporation and representatives. And in many cases, companies believe that if they are doing business with someone who holds a licence from a regulatory body such as the UKGC or Malta Gaming Authority (MGA), due diligence doesn't need to be undertaken again by the subject person or company which is a real example of the misunderstanding of the regulatory framework and expectations.

As part of its risk assessment process, the research team at Acuris Risk Intelligence carries out due diligence daily on multiple B2B relationships within the gaming sector, including regulators, vendors, suppliers, intermediaries, contractors and other service providers. As indicated by the UKGC the risk assessment process should consist of three standard stages: Identification, Analysis and Evaluation.

These due diligence investigations assist the industry in the Identification stage. In order for the customer to be well educated during the Analysis and Evaluation steps of the risk assessment, we rely on a combination of compliance solutions, proprietary data and human intelligence with access to government, media and proprietary sources.

While in some cases, due diligence has identified minor risks such as fines, we have also, in a number of cases identified unknown parties within business relationships such as beneficiaries, trustees and shadow directors. In some cases, direct links to Political Exposure (PEPs) and people with high money-laundering, reputational, cyber and additional risks were also uncovered. Those risks were critical during the risk assessment process and in the decision of our clients to accept or reject the B2B relationship with the third party.

Analysis highlights

For factual analysis of the risks associated with B2B gambling relationships, we have summarised the findings from 60 B2B Enhanced Due Diligence (EDD) reports undertaken specifically for the gaming industry. These reports cover subject companies in multiple jurisdictions, from Europe, Asia-Pacific, the Middle East, the Americas and through to Sub-Saharan Africa. The research concluded five main risks in B2B relationships:

- Reputational – risk of damage to reputation, good name, brand image or negative media coverage
- Financial – risk of loss of funds or delayed service provision
- Regulatory – risk of administrative measures, fines or revocation of licenses and additional permits
- Cyber – risk of loss key data or security breaches as a result of the B2B relationship
- Transparency – risk of non-compliance with AML, anti-terrorist financing and tax compliance requirements.

To identify these risks, the research methodology focused on uncovering any information on the third-party subject company related to:

- Beneficial ownership
- Political exposure of senior management team, members of the board of director or beneficial owner(s)
- Countries of operation and management of the third party
- Participation of the third-party in regulatory and litigation proceedings and a defendant(s)
- Negative media coverage and additional reputational risks
- Sanctions imposed by UN, EU, OFAC, Austrac, HMT and additional competent bodies
- Country-specific sources - media publications in local language, trade journals, company and court registers, government and proprietary databases.

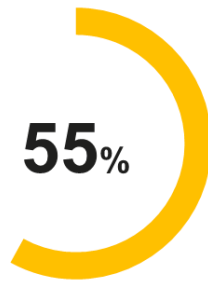
The findings of the reports concluded:

- **55% of entities show negative media coverage** of the third-party company, its directors or beneficial owner
- **26% of third-party companies are linked to PEPs**, while 8% of the due diligence reports uncovered high-ranking PEPs among the directors or owners of the third-party company
- **19%** of the cases showed links to **companies listed in the leaked database of offshore records known as Panama papers**
- **15%** of cases share a **combination of PEP and negative media risk**
- **15% of cases found a fine or injunction** imposed by the third-party company's sector regulator



PEP

In 26% of the cases analyzed PEP risk was identified



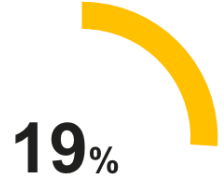
Negative media

In 55% of the cases analyzed negative media risk was identified



Regulatory and litigation

In 23% of the cases analyzed regulatory and litigation risk was identified



Panama papers

In 19% of the cases analyzed companies listed in the leaked database of offshore records known as Panama Papers was identified

Political exposure – additional details

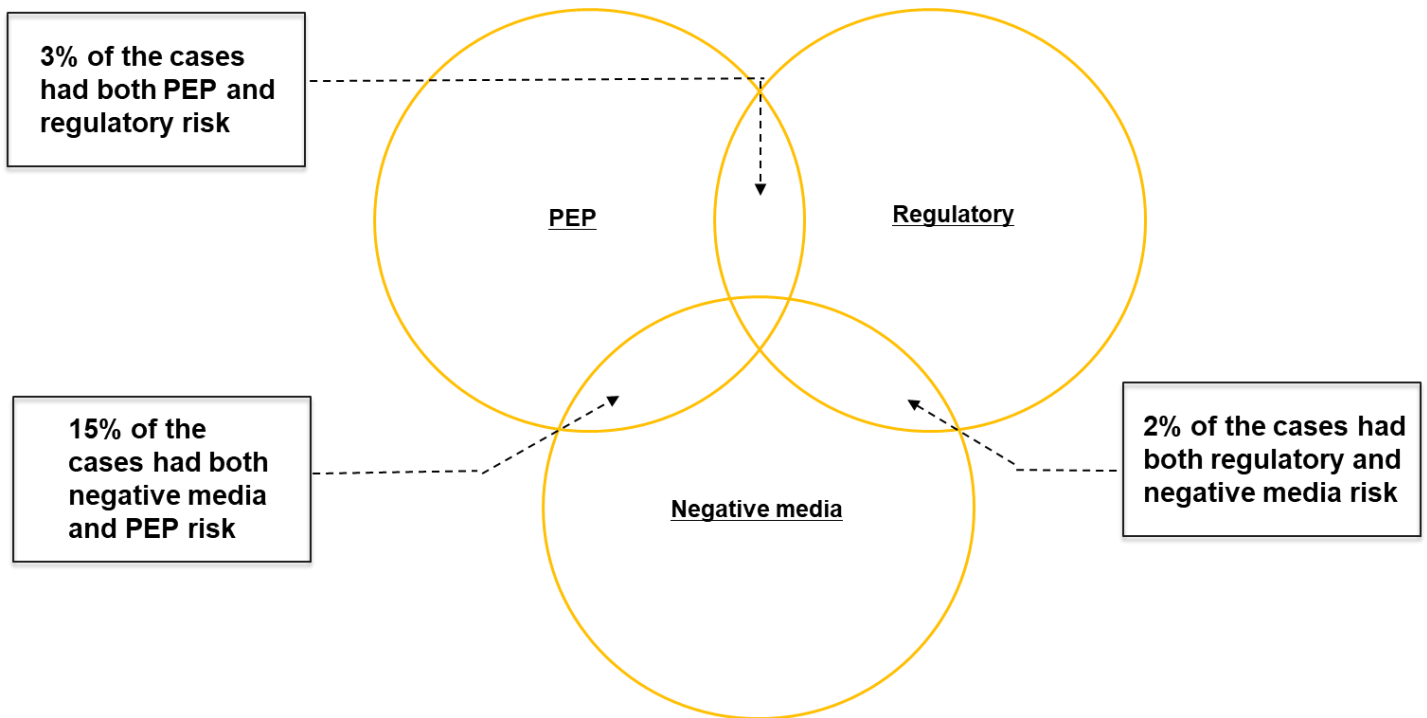
The analysis on politically exposed persons focuses on officials (other than junior officials) entrusted with prominent public functions either in a government body or international organisation, as well as their family members and close business associates.

In our analysis, we have found that 27% of all third-party companies had PEPs in their board, C-level management team or beneficial owner(s). Also, out of those PEPs, 8% were high-ranking government officials such as ministers and deputy or assistant ministers, members of parliament or of similar legislative bodies, top officials of mainstream political parties, or members of legislative and executive bodies at regional, provincial, cantonal or equivalent levels.

Negative media coverage – additional details

Negative media checks focus on people and entities identified in official, non-official and media sources as having been involved or alleged to have been involved in several distinct categories of misconduct. These include financial crime and fraud, bribery and corruption, cybercrime and other alleged offences as defined by FATF, the UN, the EU, international law enforcement agencies and regulators in the UK and the USA.

The analysis found that 15% of cases share a combination of PEP and negative media risk.



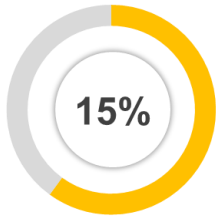
Regulatory and litigation - additional details

Apart from reputational risks, we analysed additional commercial and business information that helps gaming industry participants decide whether they should enter a business relationship with a third party. This includes regulatory, bankruptcy and litigation checks. Our regulatory checks focus on any fines and compulsory measures imposed by gaming, competition protection, data privacy, financial market and anti-money laundering bodies, and additional relevant regulatory bodies in various jurisdictions. Our litigation checks focus on civil disputes between the third-party company and any of its vendors, management or employees. They also look for criminal proceedings against key management personnel, beneficial owners or the entity itself (where the jurisdiction of interest allows for legal entities to have criminal liability).

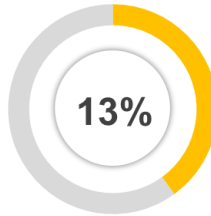
Examples of identified regulatory actions taken against a party in a B2B transaction include:

- Added to the list of illegal gambling operators after a decision of the Vilnius Regional Administrative Court
- Fined for infringement of the Romanian national and community competition law

- Violation of the National Gambling Act of 2004, which banned online gambling in South Africa
- Injunction prohibits director from making any change or action relating to his shareholdings in casinos in Morocco



Cases related to fines and injunctions



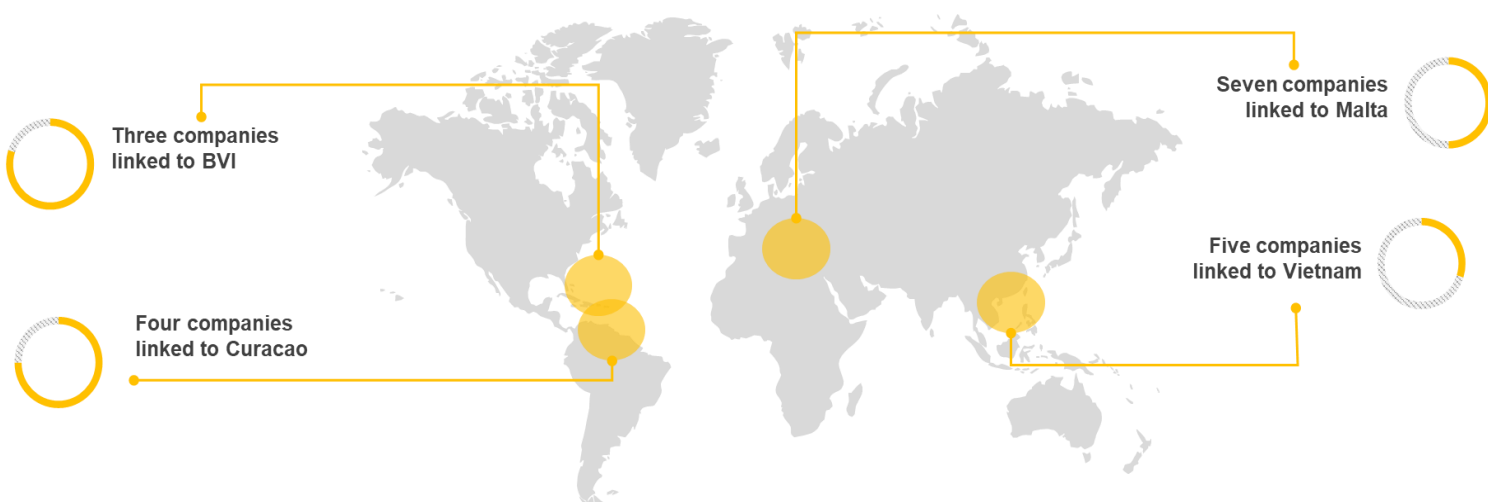
Cases related to illegal online operators list

Beneficial ownership

When it comes to beneficial ownership, in 12% of cases we found beneficial owner links to high-risk jurisdictions that were unknown to the client. Increasingly complex company structures and networks make relationships to high-risk countries hard to uncover and often require searching through multiple layers of ownership and jurisdictions. Use of offshore companies, trusts, nominee shareholders, foundations, partnerships, and other types of legal arrangements are also common.

Third-party providers associated with higher-risk countries may present a higher money laundering risk. We use FATF data and additional non-governmental organisations such as Transparency International, the Basel Institute on Governance, Freedom House and others to determine jurisdiction risks such as perceptions related to corruption, risks of money laundering and terrorist financing.

In our sample of sixty cases, we analysed multiple layers of ownership and uncovered beneficial owner links to high-risk jurisdictions that our clients were not aware of, as detailed in the map below:



Case studies

The four case studies that follow are a result of due diligence on a potential B2B relationship and illustrate all the risks we have discussed.

Case study 1 – Beneficial owner of gaming operator found guilty of illegal forex trading

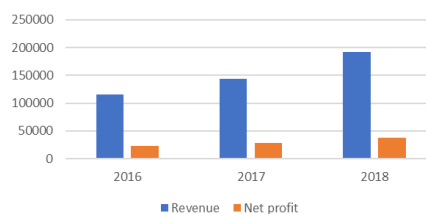
Company profile

- Company operating an online casino, incorporated in the Russian Federation
- The shareholders of the operator are two Russian individuals
- Russian business registries found more than 20 companies related to the subject company
- Insolvency investigation did not uncover any actions taken against the subject company or its subsidiaries

Regulatory

- US litigation records found the beneficial owner of the subject company was found guilty of illegal foreign currency futures trading, was ordered to repay customers and was imposed a further civil penalty.
- Russian regulatory records found the subject company committed an administrative offense by performing retail sale of alcoholic beverages without a corresponding license.
- Russian regulatory records found the subject company was brought into administrative responsibility and fined for failing to comply with the legislation regarding anti-money laundering and counter terrorism.

Financials



PEP

- No PEPs were found on the board of the operator
- BO is not a PEP

Case study 2 – Operator fined for infringement of the Romanian competition law

Overview

- Gaming solutions supplier and operator, listed on the Athens Stock Exchange
- Subsidiaries of the subject company include multiple entities across 55 countries
- Company's games library includes more than 550 games, including lotteries, sports betting, Video Lottery Terminals (VLTs)/Amusement with Prizes machines (AWPs) and racing

Regulatory action

- Romanian Competition Council (RCC) fined the subject company and three others, responsible for the development of the video lottery programme in Romania, for infringement of the national and Community competition law as a result of the implementation of a non-compete clause within the Supplier Credit Contract between the companies
- An investigation was launched by the Romanian antifraud authority against the subject company and was continued by Bucharest Court of Appeal prosecutors in 2013. The Romanian prosecutors also launched a second investigation to recover illegal income from the subject company

Case study 3 – OFAC imposed civil penalties for export violations

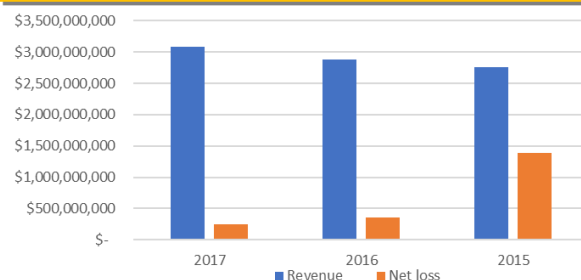
Company profile

- Company registered in Las Vegas, reported to hold all licences and permits necessary to conduct the authorised sale, lease or operation of gaming products and services in over 100 jurisdictions worldwide.
- Has multiple subsidiaries in Sweden, the UK, France, Mexico, New Zealand.
- A minority shareholder in the company (10% equity stake) is based in Hong Kong.

Regulatory

- US Department of Treasury searches identified an OFAC Civil Penalties Enforcement against an entity with the same name as the subject company for an offence related to export violations.
- The Hong Kong-based minority shareholder of the subject company is also a shareholder in an electronic payment system in Russia and Ukraine that is reportedly being used for financing criminal and terrorist activities.
- The company was a defendant in a case where plaintiffs were seeking damages of USD 335 million and injunctive relief for defendants' alleged violation of unfair competition and deceptive trade practices laws.

Financials



PEP

- One board member was former US Assistant Attorney General for Legal Policy
- One board member was former member of the District Court for the Southern District of Texas

Case study 4 – Company licensed by the Kahnawake Gaming Commission having its domains blacklisted

Overview

- Company registered in Malta
- Licensed by the Kahnawake Gaming Commission
- Owner of several domains listed on the official website of the Kahnawake Gaming Commission
- Operates five online casinos

Regulatory action

- According to an Order of the Director of the Gaming Control Authority under the Ministry of Finance of the Republic of Lithuania, one of the subject company is listed as an illegal online gambling operator.
- The State Commission on Gambling under the Ministry of Finance of the Republic of Bulgaria listed two domains, owned by the subject company as illegal online gambling websites
- The main domain of the company is listed in a blacklist of websites providing gaming services in Greece without a license
- According to a media article, one of the beneficial owners of the subject company used to provide consulting services to an online gaming brand which, according to Italian investigators, had ties to organised crime in southern Italy

Conclusion

In the gaming industry, the risks within B2B relationships is primarily driven by the inherent complexity of the business sector as a whole. As the report shows in many cases there are risks around fines imposed by regulators on the third-party company or its managers, bans on marketing campaigns and promotional materials along with civil lawsuits.

However, in some cases the risks uncovered are not obvious. They require in-depth research in local language and detailed analysis of many different aspects of the third party: corporate structure; the personal background of managers, family connections, board members and shareholders; its core business, various business licenses and permits; and its litigation and regulatory action history and additional media coverage; as well as researchers who are specialists in these areas and understand the industry nuances.

As our experience shows, unknown risks to the customer are often uncovered only after a detailed investigative and through due diligence process is completed. In some cases, the relationship will require additional monitoring and ongoing due diligence, in others, these risks can significantly change the decision as to whether the company should conduct business with the third party, or at least enter into the relationship knowing the facts to help aid business decisions.

With the ever-growing global reach of the gaming industry and complexity and prevalence of corporate structures, the need for independent and highly experienced enhanced due diligence/investigations, be it via in-country desk top research and or on the ground investigations has never been so important.

At Acuris Risk Intelligence we help gaming operators protect their brand reputation and shareholder value, and confidently support the mitigation of regulatory risk exposure through best-in-class screening & investigation practices on suppliers, clients, and third parties, to create safer and more transparent business relationships across the world.