AML Tuesday's Session #29 on:

Sector-Specific STR Typologies and Red Flag Scenarios applied in Practice

for the Casino sector

September 10, 2024

Discussion Topics

01 Reporting obligations

02 Typologies, including new and emerging typologies

03 Red flags indicators

Typologies

=

Methods and trends associated with ML/TF/PF/C

Traditional typologies

New and emerging typologies

Awareness of typologies (worldwide, in the region, country, for the sector), can **help understand risks** to which the reporting entity's business is exposed and prevent abuse of the business by criminals and their associates

Red flags/Indicators

=

Warning signs that ML/TF/PF/C may be taking place

Based on **unusual behaviour or profile** of the customer/BO, source of funds, transaction, etc.

Indicators must always be considered in **context** - the presence of an indicator does not necessarily directly raise suspicion of ML/TF-P-C, but may **prompt closer examination** to determine whether there are **grounds to file an STR.**

Both documented in publications of global bodies (e.g. FATF, Egmont Group, UNODC), regional bodies (e.g. EUROPOL, EC) and national authorities (e.g. AMSF guidance, FIU annual reports); sector associations, media & NPO reports

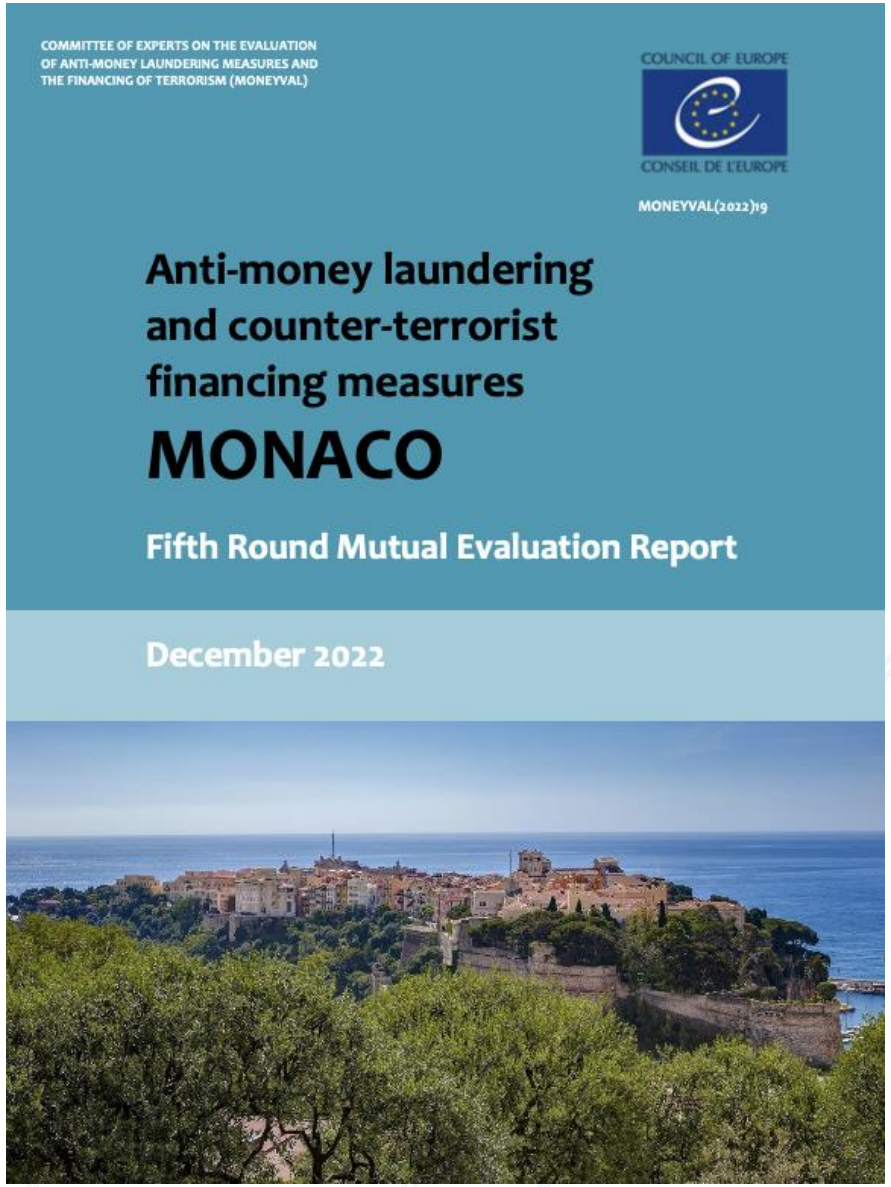
01 Reporting obligations

Monegasque legal framework

- The relevant legal obligations relating to the analysis and reporting of suspicious transactions for all reporting entities, are set out in:
  - **Art. 14 of the Law 1.362 (special examinations)**
  - **Chapter V (Art. 36 to Art. 45) of the Law 1.362 (STRs & mandatory reporting)**
  - **Art. 31 & Art. 36-2-1 of SO 2.318 (internal controls on reporting & form of reporting)**
- Professionals must file **confidentially and without delay** all transactions or attempted transactions involving sums or funds that they know or suspect to be derived from a predicate offence for money laundering or are related to terrorist financing or corruption offence, **before** the transaction is executed, or file as the report without delay **after** carrying out the transaction, giving **reasons** why it could not be filed before.

2022 MONEYVAL evaluation

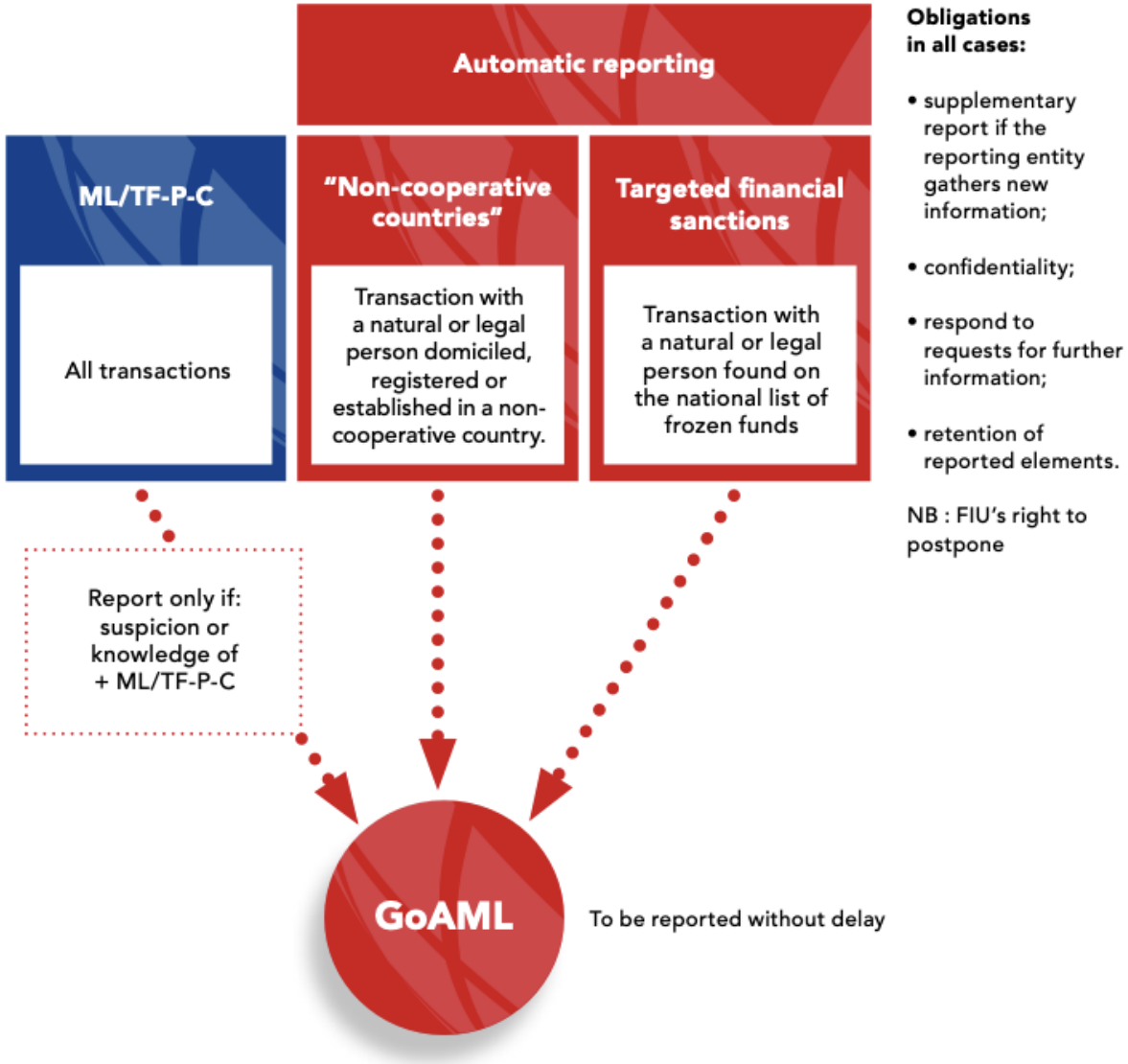
- MONEYVAL found that the **number of STRs submitted by the casino remains limited**, even though the sector accounts for the bulk of DNFBPs' customers and transactions and handle **cash** more frequently than FIs and other DNFBPs.
- MONEYVAL found the overall effectiveness of the STR reporting system in Monaco to be **low to moderate**.
- MONEYVAL recommended that the authorities should take measures to **improve the timeliness and quality of STRs**, in particular by providing guidance and additional red flags indicators, further developing the typologies, ensuring that the reporting entities understand and timely fulfil their STR obligations, and ensure that their internal audit and control departments monitor their sustainable implementation.



Examples of actions taken pursuant to MONEYVAL Recommendation

- Implementation of **GoAML platform** for STR reporting
  - Relevant instructions and training slides on the use of GoAML are published on this AMSF webpage
- **AMSF publications** providing guidance on STR obligations and red flags indicators:
  - **Short Practical Guide on STRs**, providing a brief global overview of reporting obligations
  - **Detailed Guideline on STRs**, containing more detailed explanations of reporting obligations as well as an **Annex with Indicators** for suspicions
  - **Guidance on PEPs**, in light of exposure of Monaco to proceeds of offences of corruption, including specific red flags indicators related to these areas
  - **Terrorist Financing** Awareness Guide, including an Annex with TF indicators
  - All of these publications are available in French & English at this AMSF webpage
  - **Guidance for the casino sector** (shared directly with the casino), including a section on STR obligations
- **Training** organised by AMSF & FTA, including:
  - 2023 AML Tuesdays sessions on STR reporting and Typologies & Red flags relating to TFS, TF and PF; slides are available on this AMSF webpage
  - In-person training on "Effective STR reporting" from 13-16 November 2023; slides are available on this AMSF webpage

Some key points from guidance on STR obligations



AMSF Supervisory Findings on DNFBPs - 2023

Findings on ongoing monitoring and identification of suspicious activity

- Ongoing monitoring not conducted
- No risk-based approach to monitoring
- Number of false positive alerts not clear
- Inadequate screening (country lists) & Infrequent or incomplete screening of customers and transactions
- Failure to identify repeated transactions even if obliged entities are diligent regarding limits on cash payments and are aware of their obligation in this respect
- Failure to update customer profile and CDD with details received during assessment or investigations

Findings on Suspicious Transaction Reporting

- Failure to report or low quality reporting
- Failure to submit additional information on already submitted STRs
- The extent of the reporting obligation is not always fully understood
- Inordinate delays in reporting

June 2024: Monaco grey-listed by FATF

To be removed from the list, the FATF expects to see the **effects of these efforts** and to note **improvements in the quality and timeliness of STRs filed in practice**:

MONACO

In June 2024, Monaco made a high-level political commitment to work with the FATF and MONEYVAL to strengthen the effectiveness of its AML/CFT regime. Since the adoption of its mutual evaluation report (MER) in December 2022, Monaco has made significant progress on several of the MER's recommended actions including by establishing a new combined financial intelligence unit (FIU) and AML/CFT supervisor, strengthening its approach to detecting and investigating terrorism financing, implementing targeted financial sanctions and risk-based supervision of non-profit organisations. Monaco will continue to work with FATF to implement its action plan by: (1) strengthening the understanding of risk in relation to money laundering and income tax fraud committed abroad; (2) demonstrating a sustained increase in outbound requests to identify and seek the seizure of criminal assets abroad (3) enhancing the application of sanctions for AML/CFT breaches and breaches of basic and beneficial ownership requirements; (4) completing its resourcing program for its FIU and strengthen the quality and timeliness of STR reporting; (5) enhancing judicial efficiency, including through increasing resources of investigative judges and prosecutors and the application of effective, dissuasive and proportionate sanctions for money laundering; and (6) increasing the seizure of property suspected to derive from criminal activities.

AML Tuesdays session of 17/09/2024 will provide further information on the FATF's decision to grey-list Monaco and the ICRG follow-up process and actions to be implemented to exit the list

02

Typologies, including new and emerging typologies

Common ML typologies involving casinos

Examples of some **“classic”, well-known techniques** in scenarios reported worldwide whereby criminals and their associates use transactions in casinos to launder funds:

- **Cash-in cash-out** – the simplest, most typical method of ML at a casino, also often used in combination with other techniques
- **Structuring/smurfing** (breaking up a large amount of cash into smaller transactions in order to minimise suspicion and evade threshold reporting requirements) & **refining** (exchanging low denomination for high denomination currency)
- Use of **‘mules’ or collaborators** that buy chips on behalf of criminals for illicit cash
- **Buying winnings/chips** from legitimate players, offering them cash above their value.
- **Junkets and introducers:** arrangements between hosting casino and introducer/junket operator to facilitate gambling by high-wealth players, including through VIP programmes and pooled accounts. Also related to forms of **junket financing**, including offsetting (system of debits and credits in different countries used to offset wins and losses against the original amount deposited) or loan sharking.
- Abuse of leniency, high level of turn-over and incentives applicable to **VIP customers and high rollers**
- **Criminal infiltration** of casinos and **bribery/collusion** with managers and staff to turn blind eye, avoid questions and reporting
- **ML schemes involving loan sharking/usury**, combined with offsetting/hawala-like arrangement: see next slides
- Abuse of **casino accounts/player accounts**, see slides further on.
- **Collusion between players**, e.g. typology of **intentional gambling losses**: proceeds of crime are brought into casinos and deliberately lost e.g. in a card game in a way that **benefits an accomplice** who acts as another player in the same game

Loan sharking/usury and ML

- Loan sharking leads to proceeds of crime but can also be used in ML schemes
- Loan sharking consists of illegal schemes to **loan (dirty) cash money** to individuals at high interest rates, sometimes collected under blackmail or threats of violence.
- Loan sharks may be financed and supported by **organised crime networks** who are also involved in ML activities; **junkets** may also act as loan sharks.
- In casinos, a loan shark usually preys on **high-roller players** and individuals who are **problem gamblers** or have financial struggles or are unable or unwilling to seek legal forms of credit. The loan can be extended in cash or in chips.
- Players can be required to pay-back their loan and losses via bank-deposits into (foreign) bank accounts controlled by the criminals ("**offsetting arrangements**"/"**mirror transactions**"), leading ultimately to the loan sharks receiving laundered money in non-cash form.
- Persons in debt to loan sharks may also be coerced into **assisting with ML schemes** within the casino, e.g. acting as mules to acquire chips with dirty money or open player accounts as frontmen.

Loan sharking/usury and ML – typology applied in practice

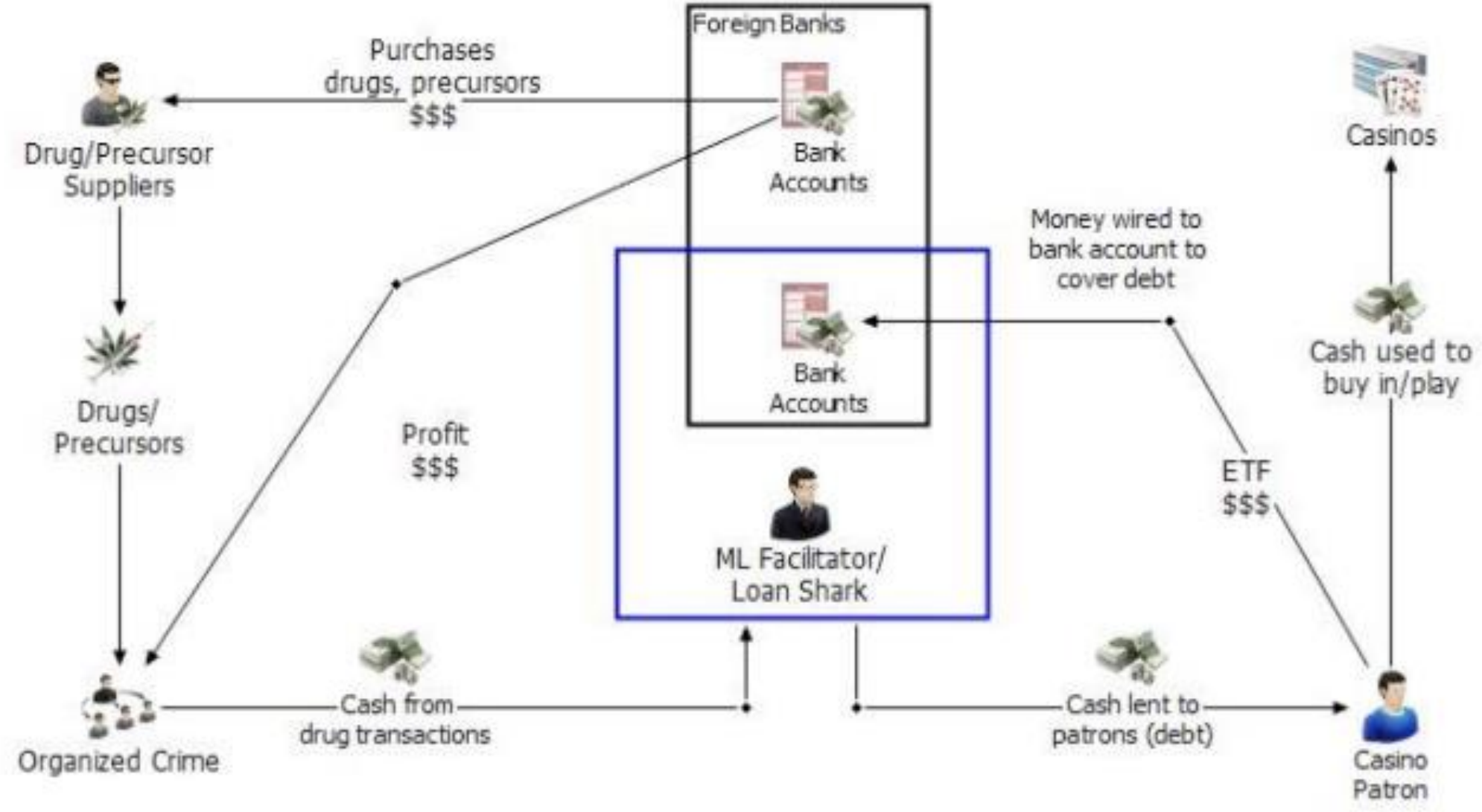
Canada: "The Vancouver Model", mixing cash-in/cash-out, loan sharking and hawala ML techniques

"Investigation by IPOC … to date indicates that **groups of loan-shark "facilitators" are constantly present in and around the casinos**, ready to supply **large quantities of cash** to these **high-roller players**. These high-roller players **typically pay-back their losses via bank-deposits in the PRC or Hong Kong**, which are ultimately brought back to Canada by the loan-sharks (in non-cash form) as "legitimate" money. This is often done by international money-laundering groups, using a **"hawala"** [sic] style of debt-settlement, where a debt in Canada can be paid-back with a corresponding credit overseas (or vice-versa).."

"The enormous quantities of illicit cash that came to be accepted in British Columbia's gaming industry were distributed to casino patrons as part of the Vancouver model money laundering typology. While these funds were genuinely gambled and often lost, their **acceptance facilitated the laundering** of this illicit cash by enabling criminal organizations to dispose of it and be **repaid in other forms in other jurisdictions**, thereby transferring the funds to another part of the world, converting them into a different form, and obscuring their illicit origins."

Source: Report of the Cullen Commission's Inquiry into Money Laundering in British Columbia (June 2022)

Figure 10. 'Vancouver model' for money laundering through British Columbia's casinos



ML through abuse of casino accounts

- Casino accounts provide criminals further opportunities to (attempt to) laundering crime proceeds
- Many casinos offer their customers deposit accounts and lines of credit with less scrutiny and CDD requirements than financial institutions.
- The frequent movement of funds between financial institutions and casinos, or between casino accounts held in different casinos may be vulnerable for money laundering.
- Accounts can be used and abused to launder money in various ways, including through deposits of illicit money into accounts; the use of multiple sources or aggregation to fund accounts; the requesting of pay-outs (potentially with minimal gaming activity) into other accounts; account-to-account transactions (where permitted), etc.

Abuse of accounts – typology applied in practice

Australia: Crown Resorts Group case on the facilitation of ML through accounts of entities associated to the casino and player accounts

- Crown Resorts has three operating subsidiaries holding casino licenses: **Crown Melbourne**, Burswood Nominees Ltd as trustee for the Burswood Property Trust (**Crown Perth**), and Crown Sydney Gaming Pty Ltd (**Crown Sydney**),
- In 2019, Crown Resorts became subject of allegations that two private companies set up by Crown Resorts (**Southbank**, a wholly owned subsidiary of Crown Melbourne & **Riverbank,** a subsidiary of Burswood Limited, which operates Crown Perth), with Crown executives as directors, were used to facilitate the laundering of proceeds of crime.
- The companies did not carry on business but simply **operated bank accounts to receive casino patrons' funds**, reportedly to "afford its international patrons privacy".
- Initially, both Southbank and Riverbank held bank accounts with HSBC. In 2013, HSBC decided to discontinue its relationship with the entities and they found other Australian banks.
- Crown circulated the details of the Southbank and Riverbank accounts to its patrons and advised them that, when making a deposit, the depositor should reference the Crown identification number of the patron so that the **patron's deposit account could be credited accordingly**. When funds accumulated in the Southbank and Riverbank accounts, they would be 'swept' into Crown bank accounts at regular intervals. Hundreds of millions of dollars flowed through the Southbank and Riverbank accounts annually.

Abuse of accounts – typology applied in practice - *continued*

Australia: Crown Resorts Group case on the facilitation of ML through accounts of entities associated to the casino and player accounts

- Despite Crown directing patrons that the Southbank and Riverbank accounts would not accept **transfers from companies**, when such transfers were made, they were in fact accepted and credited to the associated patron's account.
- Further, the **aggregation** of multiple deposits for a single patron deposit account into a single entry by cashier staff into the electronic customer relationship management system used by Crown meant that AML staff were unable to identify the fact of aggregation, or the exact source, timing, number and nature of the individual deposits that constituted the aggregated amount.
- Indications that money laundering was, or was likely to be, occurring through the Southbank and Riverbank accounts from at least January 2014, including indicators for **structuring** and **failures** of the Crown officers to provide their bankers with clear information and evidence of **source of funds checks**, ultimately lead to the new banks also closing the companies' accounts (but some only as late as 2019).

Source: Report of the Finkelstein Inquiry/Royal Commission into the Casino Operator and Licence (October 2021)

New and emerging typologies and trends in typologies

- Global and regional bodies such as FATF periodically publish **reports describing new and emerging ML/TF typologies** observed worldwide as well as **trends in known ML/TF typologies**, e.g. changes in the regional scope, known actors, scale or risk level of the techniques.
- Reporting entities should keep themselves informed about such publications and determine which typologies can be **relevant in the context of their own geography, sector, business, customer profile and activities**
- The reporting entity should monitor evolving risks on a continuous basis to determine whether there is a need to update its policies and procedures in order to adapt to the risks, e.g. whether there is a need to **add new red flags to its internal list of indicators** for potentially suspicious activity on the basis of such typology reports

Example 1 of recent publication on typologies

- CBI/RBI programmes attract an array of clients, many of whom have gained their assets legitimately and have benign intentions.
- However, they can also be abused by criminals who seek to launder and conceal proceeds of crime or commit new offences, undermining these programmes' intended objectives.
- **As the popularity of investment migration programmes has grown, the risk of illicit actors utilising these programmes to their advantage has also increased.**
- CBI programmes are particularly vulnerable, because they allow illicit actors more global mobility and possibilities to disguise their true identity by obtaining new ID documents
- High-risk individuals can also use a frontperson (family member or associate) to make the application for CBI/RBI. This typology is particularly salient in the case of PEPs/corrupt actors/sanctioned individuals.

Misuse of CBI/RBI – typology observed in Europe & Monaco

From **European Commission's 2022 supra-national risk assessment (sNRA) for ML/TF**, chapter on CBI/RBI:

- The sNRA cites numerous examples of jurisdictions with **CBI schemes that have attracted wealthy people known or suspected to be involved in ML schemes**, including Malta, Cyprus, and Caribbean jurisdictions.
- Since the imposition of EU and U.S. economic sanctions, visa bans and asset freezes on Russia following its invasion of Ukraine in 2014, there has been **a surge in Russian applications for investor citizenship schemes worldwide** and in Europe (Cyprus, Malta)**;** this has given rise to the **risk of sanctions evasion** in addition to the potential laundering of illicit funds:
- **Proliferation financing/sanctions evasion risks:** North Korean nationals have also previously managed to obtain alternative passports (notably in **Caribbean countries**), which they use to conduct business worldwide.
- The EC concludes that the estimated risk level of ML for CBI/RBI schemes is **VERY HIGH**.

In **Monaco**, the FIU has also come across **scenarios** that could be linked to the misuse of CBI/RBI for ML purposes

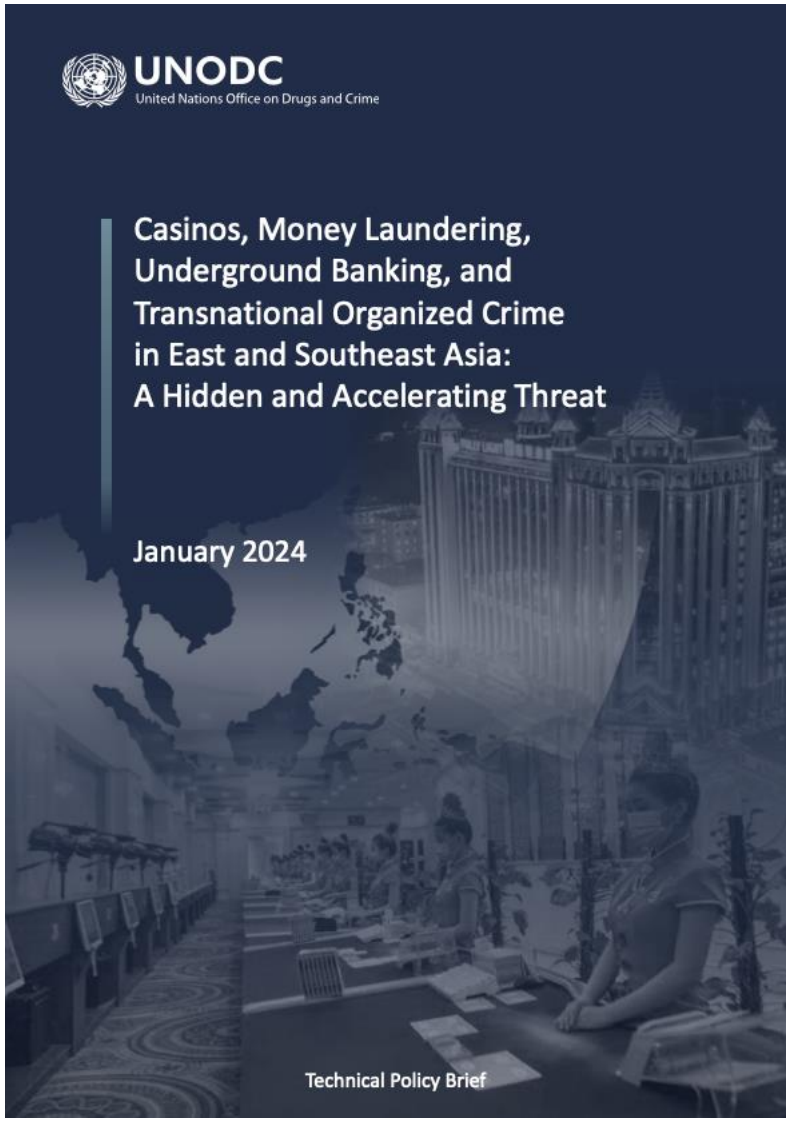
Misuse of CBI/RBI – EDD, monitoring and red flags

- The OECD maintains an overview of jurisdictions with high-risk CBI/RBI schemes
- The EU sNRA also provides examples of jurisdictions with schemes that are controversial or known to be exploited (see previous sheet)
- Reporting entities should subject customers with citizenship/residency from jurisdictions with high-risk CBI/RBI schemes to **enhanced checks**, e.g. to determine:
  - whether they benefited from CBI/RBI schemes;
  - whether they have changed their identity in the course of the CBI process;
  - ensure that all their names, all their nationalities and passports are disclosed as part of CDD etc.,

  and **closely monitor/scrutinize the transactions of persons who benefited from such schemes**

⚑ A customer benefited from a foreign CBI scheme or a RBI scheme in a foreign jurisdiction with limited transparency, screening and monitoring measures for investors

Example 2 of recent publication on typologies



- As demonstrated by cases analyzed for this report, **casinos and junkets (both land-based and online) represent a critical piece of the underground banking and ML infrastructure**, serving the needs of transnational OCGs operating in the East and Southeast Asian region, who are also observed in recent years to be further expanding their activities **globally (including across Europe,** as reported mostly through **online gaming).**
- Casinos and related businesses have proven both capable and efficient in **moving and laundering massive volumes** of state-backed fiat as well as cryptocurrencies undetected; creating channels for effectively integrating billions in criminal proceeds into the formal financial system.
- **Recent law enforcement action has also demonstrated the scale at which some junket operators have been able to serve as international bank-like entities,** providing a variety of underground financial services including credit issuance, currency exchange and multi-currency payment and settlement solutions, remittances and extra-legal debt collection mechanisms which have been exploited by organized crime - authorities and experts have identified **similar methods to the Vancouver Model exploited by organized crime networks operating though casinos in Australia and East and Southeast Asia.**

03 Red flags indicators

POINTS TO WATCH

Reporting entities must adopt their own indicators in the light of their activity and risk profile.

The mere presence of an indicator is not necessarily grounds for suspicion of ML/TF-P-C, but may prompt surveillance and closer examination. Conversely, a number of indicators may be grounds for suspecting ML/TF-P-C.

Indicators must always be considered in context.

Indicators are points of attention that arouse suspicion or allow the reporting entity to detail its suspicions about a given transaction. The AMSF proposes a non-exhaustive list of indicators, which can be consulted on its website.

The next slides contain **non-exhaustive examples of indicators**

Reporting entities should develop their own internal lists of red flags, tailored to their **own activities and profile:** products and services, customer base, transaction sizes, etc.

AMSF AUTORITÉ MONÉGASQUE DE SÉCURITÉ FINANCIÈRE

Annex:

Indicators for suspicions

AMSF AUTORITÉ MONÉGASQUE DE SÉCURITÉ FINANCIÈRE

Summary

I. Cross-sectoral indicators 3
General indicators 3
Specific indicators for terrorist financing 6
Specific indicators for corruption and laundering of proceeds of corruption 8
II. Indicators for financial sectors 10
Retail banks 10
Private banking 12
Asset management companies 13
Life insurance brokers & agents 16
Bureaux de change 17
Pawnbrokers 18
III. Indicators for DNFBP sectors 19
Real estate sector 19
Casino sector 22
Legal professionals and accountants 24
TCSPs 29
Business centers 30
Dealers in Precious Metals & Stones, Jewellers and Watchmakers 31
Yachting/chartering sector and Motor vehicle sector 32
Arts & antique dealers and Auction houses 32
Sports agents 33

General red flags indicators across sectors

Indicators relating to **customers**

Indicators relating to **transactions & payment methods**

Geographical indicators

Indicators relating to **distribution channels**

Examples of indicators relating to **customers:**

- The customer is highly reluctant, refuses to provide information, or provides minimal, unclear or inconsistent information, or seemingly fictitious information, in relation to his/her identity, their business activities, source of funds etc.
- The customer tries to persuade the (employee of the) reporting entity to not keep records of any documents that it has shared
- The customer has repeatedly changed financial institutions/bank accounts in a short period of time and cannot give a plausible reason for this

Corruption red flags indicators

Indicators relating to **PEPs** *(see also the indicators in the PEP guidance)*

Other indicators relating to corruption

Examples of indicators relating to **PEPs:**

- Customer or beneficial owner is a PEP who receives a modest official salary, but who seeks to conduct high-value transactions, without any apparent legitimate additional income (business interests, inheritance etc.)
- Transactions involve funds moving to and from countries (e.g. location of bank account, issuing country of credit card) with which the PEP do not appear to have legitimate ties
- PEP receives abnormal cash deposits in their accounts

AMSF AUTORITÉ MONÉGASQUE DE SÉCURITÉ FINANCIÈRE

Annex:

Indicators for suspicions

AMSF AUTORITÉ MONÉGASQUE DE SÉCURITÉ FINANCIÈRE

Summary

I. Cross-sectoral indicators 3

General indicators 3

Specific indicators for terrorist financing 6

Specific indicators for corruption and laundering of proceeds of corruption 8

II. Indicators for financial sectors 10

Retail banks 10

Private banking 12

Asset management companies 13

Life insurance brokers & agents 16

Bureaux de change 17

Pawnbrokers 18

III. Indicators for DNFBP sectors 19

Real estate sector 19

Casino sector 22

Legal professionals and accountants 24

TCSPs 29

Business centers 30

Dealers in Precious Metals & Stones, Jewellers and Watchmakers 31

Yachting/chartering sector and Motor vehicle sector 32

Arts & antique dealers and Auction houses 32

Sports agents 33

Indicators for the casino sector

Indicators related to gambling

Indicators related to buy-ins and pay-outs

Indicators related to player accounts

Indicators related to cash

Indicators related to currency exchange

Other indicators

Examples of indicators included in the Annex

Sample indicators relating to **player accounts**:

- Account activity with little or no gambling activity
- Dramatic or rapid increase in size and frequency of transactions for regular account holder
- Casino accounts are attempted to be funded by transfers from corporate accounts
- (Attempts for) Deposits into casino account using multiple payment methods or multiple individuals
- Requests to transfer funds into third party accounts or corporate accounts

Sample indicators relating to **cash**:

- Purchasing of casino chips or funding of player account with large amounts of small denomination bills
- Customer appears to attempt to avoid the filing of a cash transaction slip by structuring/breaking up the transaction
- Customer engages in frequent cash transactions just under the thresholds that apply for certain due diligence measures applied by the casino or that apply for maximum cash transactions

Fictional case study: Application of red flags scenario in practice

- A customer from India, Mr X, frequently travels to Monaco for business and leisure and has a **player account** with the casino, that is regularly fed through personal card and bank account transactions from a US bank.
- The declared source of funds is the money that Mr X receives as salary for directorship of a real estate investment fund in Asia and dividend through investments in REIFs worldwide, incl. the US.
- Given the **geographic and sectorial risks** associated with this customer, the customer is classified as medium-high risk and the casino has obtained additional CDD information in the form of salary slips and proof of dividend payments, demonstrating a total income equalling approx. €2 million per year.
- After one year of being a customer, the casino's monitoring system **alerts** to a sudden increase in the level of funds deposited into Mr X's accounts and also a change in bank account, now originating from a personal bank account in Malta.

Fictional case study *(continued)*

Red flags immediately identified by the staff member analysing the alert:

- Large and rapid increase in size of transactions for regular account holder
- Change in account used to deposits funds into player account
- New location of origin of the funds not known to be linked to the customer
- Link to higher-risk jurisdiction for abuse of CBI/RBI programmes

- Following the alerts and the detection of these red flags, on the basis of the casino's internal procedures, the back office decides to collect further information in the context of a **special examination** into the customer and his transactions.

Fictional case study *(continued)*

- Upon enquiries as to the **source of funds** for the increased deposits and the reason for change in bank account location, Mr X declares that he has recently invested into **new businesses** generating high levels of dividend and that he has obtained **Maltese residency** thanks to the acquisition of real estate in Malta and therefore started banking in Malta.
- Mr X however repeatedly **fails to provide documentation** corroborating his new income sources and does not want to reveal the names of the businesses in Malta that he is associated to, which is **inconsistent** with his previous cooperative manner when providing information on the businesses that he is associated with.
- The staff informs him that, as long as the update of CDD information on the source of funds is not completed, they will suspend the use of the account.
- In response, Mr X requests to **close his account** and to transfer the money into yet another bank account, this time in India, held in the name of his wife.

Fictional case study *(continued)*

Additional red flags identified through the special examination:

- Customer has benefitted from a high-risk RBI scheme
- Change in customer behaviour and willingness to cooperate; customer is reluctant or unable to provide clear information and corroborating documents on the SoF
- Customer requests closure of account in response to repeated CDD requests
- Request to reimburse funds to another account than the source account

Hence, following the review of the special examination, before going ahead with closing the account and transferring the money back to the customer, the reporting officer decides to **file an STR with the FIU:**

- Describing all of the red flags identified;
- Sharing all of the CDD information on Mr X, including account numbers, and explaining missing information;
- Explaining the reasonable grounds for suspicion that the funds recently transferred into the player account originate from criminal activity;
- The casino also mentions that there is no exact prescribed period to pay back the funds but they would welcome timely feedback in order to know whether and to which account they can pay out.

Fictional case study *(continued)*

- Upon receipt of the STR and initial analysis, **the FIU orders the casino not to proceed with the pay-out, so that it has time to analyse, confirm or refute the suspicions** and disseminate the results of the analysis to the competent authorities in Monaco or foreign authorities if needed.
- As part of the analysis, the FIU sends information requests to counterparty FIUs in India, the US and Malta.
- Through their responses, it is determined that **Mr X is one of the directors and minority shareholders of the Maltese healthcare company ABC**. ABC, and the US company that is its main shareholder, as well as persons associated to these companies, are subject to recently opened **preliminary investigations in Malta and the US in relation to corruption.**
- ABC obtained lucrative contracts for the private operation of three Maltese hospitals, recently after being established and with no prior record in the healthcare business. It is suspected that the public officials deciding on the deal and the UBOs of ABC have **colluded** with a **conspiracy to embezzle** the funds. There are further indications that Mr X has obtained his residency in Malta also thanks to his **connections to politicians.**

Fictional case study *(continued)*

- In the meantime, the casino must manage the relationship with Mr X in order to avoid tipping him off as to the fact that an STR has been filed and that the transaction is being withheld.
- Mr X reverts back to the casino as to why his funds have not yet been transferred back.
- The staff indicates that under their internal procedures, they do not pay out to third party accounts and that they would need to transfer the money back to the US or Malta accounts that Mr X has used.
- Mr X claims that this is not possible since that he has already closed those accounts in the meantime and insists that the money is transferred to his wife's bank account in India.

The casino decides to **file an additional STR** to inform the FIU of **the new red flag identified**:

⚑ Alleged closure of bank accounts associated with the customer, without clear explanation.

The FIU acknowledges receipt of the additional information and will **instruct the casino as to the further course of action**, e.g. domestic authorities can obtain a court order to extend the suspension of the transaction and freeze the account within Monaco, or order the funds to be transferred back to one of the (monitored) accounts of the customer/his wife, with a view of enabling foreign authorities to freeze, seize and recover the funds.

FINANCIAL TRANSPARENCY ADVISORS

Thank you for your time

Financial Transparency Advisors GmbH
Zieglergasse 38/7/1070 Vienna, Austria

Phone: +43 1 890 8717 11

www.ft-advisors.com

http://www.ft-advisors.com

Next Session:

17.09.2024

Topic:

ICRG Discussion

Today's Host: Tamar Goderdzishvili

Today's Presenter: Suzanna van Es