SA26-1

FIAU | Financial Intelligence Analysis Unit Malta

The Landscape of Organised Crime in Malta: An FIAU Perspective

A STRATEGIC ANALYSIS

Published June 2026

Illustrative Summary

YEARS UNDER REVIEW

2021-2024

THIS REVIEW IS BASED ON

540

suspicious reports related to organised crime

KEY REPORTING SECTORS

Remote Gaming Operators

Credit Institutions

Financial Institutions – Electronic Money

Casino Licensees

Virtual Financial Assets Service Providers

DISSEMINATIONS

494

Disseminations to Foreign Counterparts

185

Disseminations to the Malta Police Force (MPF)

RED FLAGS LEADING TO SUSPICION

Adverse Media

Unknown SOF/SOW

Concerns Surrounding Transactional Activity

Uncooperative Customer

Suspected Beneficial Ownership Concealment

INTERNATIONAL VS DOMESTIC ORGANISED CRIME GROUPS (OCGs)

Highlighting key Suspected Predicate Offences most commonly identified in connection with organised crime activity.

International OCGs

1. Drug Trafficking
2. Fraud
3. Robbery & Theft

Domestic OCGs

1. Tax Evasion
2. Fraud
3. Drug Trafficking

Table Of Contents

Introduction

Organised criminal groups pose a significant risk to the financial system and society as a whole, engaging in a range of illicit activities including drug trafficking, human smuggling and extortion and subsequently utilising the financial system to launder the proceeds of their criminal activities.

This paper aims to raise awareness towards key money laundering trends, patterns and red flags frequently encountered by the FIAU in relation to these groups. The information provided in this paper is intended for general guidance purposes only and should not be considered as binding or exhaustive. As such, it should be noted that red flags and behavioural patterns should be assessed collectively and in context, as potential indicators of suspicious activity related to money laundering or terrorist financing, rather than as conclusive evidence.

Reporting entities are encouraged to quote the code outlined in this guidance document (SA26-1) within any suspicious reports submitted as a result of the guidance of this document.

1. Defining Organised Crime

The Council Framework Decision 2008/841/JHA of 24 October 2008[1] defines a 'criminal organisation' as:

> *'a structured association, established over a period of time, of more than two persons acting in concert with a view to committing offences which are punishable by deprivation of liberty or a detention order of a maximum of at least four years or a more serious penalty, to obtain, directly or indirectly, a financial or other material benefit'*

Furthermore, the concept of a 'structured association' within this definition is further clarified as:

> *'an association that is not randomly formed for the immediate commission of an offence, nor does it need to have formally defined roles for its members, continuity of its membership, or a developed structure.'*

Additionally, even though Article 83A of the Criminal Code[2] (Chapter 9) does not provide a direct definition of a 'criminal organisation', its wording functions as a working definition in a Maltese court of law by making it an offence to form, fund or join "an organisation of two or more persons with a view to commit criminal offences". Article 83A sets out the core features that define a criminal organisation.

1.1 Domestic and International Organised Crime

The FBI defines international (or transnational) organised crime groups (OCGs) as entities whose defining characteristic is their ability and propensity to operate beyond national borders. These groups, formed by individuals engaging in illicit activities, possess a structural design that inherently transcends national boundaries.

1 Source: Council of the European Union. (2008). Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008F0841

2 Source: Malta Criminal Code. (1854). Criminal Code, Chapter 9 of the Laws of Malta. https://legislation.mt/eli/cap/9/eng/pdf

They exhibit diverse organisational forms, from rigid hierarchies to flexible networks and cells, and readily adapt to changing circumstances[3]. Organised crime groups are typically considered domestic in nature, provided that their operations are confined to a single jurisdiction. Therefore, the moment a criminal group's crimes, control or money flows extend abroad, it is typically considered international.

3 Source: Federal Bureau of Investigation. (n.d.). Transnational Organised Crime. https://www.fbi.gov/investigate/transnational-organized-crime

2. Report Analysis

2.1 Sector Analysis

Between 2021 and 2024, a total of 540 suspicious reports related to organised crime were analysed for the purposes of this study, with no significant fluctuations observed across the years. Table 1 below displays the top five sectors submitting these reports, along with their respective percentages:

Sector	Percentage (%)
Remote Gaming Operators	31%
Credit Institutions	17%
Financial Institutions – Electronic Money	8%
Casino Licensees	8%
Virtual Financial Assets Service Providers	6%

Table 1: Percentage of OCG Reports by Sector

Through further analysis, it was noted that remote gaming operators were the primary submitters of reports linked to international organised crime groups, submitting approximately 50% of all reports where international OCGs were identified[4]. Conversely, credit institutions are observed as positioned to identify OCGs' related activities taking place in both international and domestic contexts. In fact, 25% of reports involving both domestic and international OCGs were reported by credit institutions.

This highlights the overall exposure of the remote gaming sector to international organised criminal groups, whilst credit institutions appear to have a strong capacity to detect illicit activities which feature elements of both domestic and international organised crime.

4 This figure is based on the data available at the time of analysis; however, it is likely understated due to inherent data constraints.

Table 2 outlines the top five reporting sectors for OCG-related reports, showing each sector's contribution to the overall volume of reports involving domestic, international, and criminal groups operating both domestically and internationally, over the period of review.

Sector	Both Domestic and International OCG	Domestic OCG	International OCG
Remote Gaming Operators	10%	25%	48%
Credit Institutions	25%	14%	25%
Financial Institutions – Electronic Money	5%	12%	2%
Casino Licensees	15%	11%	2%
Virtual Financial Assets Service Providers	5%	6%	6%

Table 2: Percentage of OCG Reports by Sector and Exposure

2.2 Outcome of Reports

When analysing the outcomes of the reports used in this analysis, approximately 29% were disseminated to the Malta Police Force (MPF). Additionally, 19% of MPF disseminations were linked to domestic criminal organisations or had connected elements, whilst the remaining 10% related purely to international organised crime groups.

A further 10% of reports led to disseminations to other national authorities, while 53% were shared with foreign counterparts. It is to be noted that approximately 20% of these reports relating to organised crime were finalised with no further dissemination.

Furthermore, Table 3 below presents the top five sectors submitting reports and the proportion of disseminations originating from these reports[5]:

Sector	Dissemination to MPF	Disseminations to National Counterparts (Excl. MPF)	Dissemination to Foreign Counterparts	No Further Disseminations
Remote Gaming Operators	5%	2%	68%	28%
Credit Institutions	65%	31%	39%	12%
Financial Institutions – Electronic Money	36%	9%	56%	18%
Casino Licensees	14%	10%	67%	21%
Virtual Financial Assets Service Providers	18%	3%	65%	24%

Table 3: Disseminations Resulting from Reports by Top 5 Sectors

Despite being the leading sector in terms of report submissions related to OCGs, the remote gaming sector's reports were among the least likely to be disseminated to the MPF, with only 5% resulting in a dissemination to local law enforcement authorities. This is in stark contrast to the 65% dissemination rate for reports submitted by credit institutions, underscoring the varying nature of these reports. Taking into consideration other key reporting sectors, 36% of reports submitted by e-money financial institutions led to disseminations to the MPF, whilst reports submitted by virtual financial assets service providers resulted in an 18% dissemination rate.

5 The percentages do not add up to 100% since a report may have been finalised with multiple disseminations to various counterparts.

It is important to note that reports submitted by the remote gaming sector tend to have a minimal connection to Malta when compared to reports submitted by credit institutions. To this extent, about 68% of reports by the gaming sector are disseminated to foreign counterparts. A similar trend is observed in reports submitted by casino licensees and virtual financial assets service providers, with 67% and 65% of reports, respectively, resulting in disseminations to foreign counterparts.

2.3 Disseminations to Foreign Counterparts

As a result of suspicious reports received from 2021 to 2024, the FIAU disseminated 494 reports to its international counterparts linked to suspected money laundering (ML) stemming from organised criminal activity. The main receiving counterpart was the Italian FIU, followed by the FIUs of Germany, the United Kingdom, Lithuania and Canada, respectively.

Counterpart	Percentage of disseminations resulting from OCG reports received between 2021 - 2024
FIU Italy	19%
FIU Germany	5%
FIU United Kingdom	5%
FIU Lithuania	4%
FIU Canada	4%

Table 4: Top Recipients of Foreign Disseminations

Based on the findings outlined in the above table, the FIAU undertook further analysis of those reports concerning organised criminal activity which resulted in disseminations to the top foreign counterparts.

The subsequent findings are included below:

Reporting Sectors Linked to Top FIU Disseminations

FIU Italy	FIU Germany	FIU United Kingdom
40% of disseminations originated from reports submitted by credit & financial institutions, with a further 26% of disseminations originating from reports submitted by casino licensees. The remainder of reports stemmed from various sectors including trustees and fiduciaries and remote gaming amongst others.	33% of reports originated from remote gaming operators, 26% from electronic money institutions and an additional 26% from credit institutions.	44% of reports originated from credit & financial institutions. A further 33% of reports were received from crypto asset services providers, indicating a potential trend where individuals with connections to the United Kingdom were potentially attempting to launder illicit funds linked to OCGs, using virtual financial assets.

Report Triggers

FIU Italy	FIU Germany	FIU United Kingdom
• Unknown source of funds/wealth • Unexplained/inconsistent transactional activity • Adverse media • Activity falling outside customer's expected profile. • Uncooperative customer	• Unknown source of funds/wealth • Unexplained/inconsistent transactional activity • Adverse media • Uncooperative customer • Unnecessarily complex structures	• Unknown source of funds/wealth • Unexplained/inconsistent transactional activity • Funnelling of funds • Adverse media • Uncooperative customer

Products Utilised

FIU Italy

- Bank & e-Money Accounts – 48%
- Gaming Products (primarily table-based) – 40%
- Cash Products – 19%
- Debit/Credit Cards – 14%

FIU Germany

- Bank and e-Money Accounts – 67%
- Payment Services – 22%
- Debit/Credit Cards – 19%
- Gaming Products – 19%

FIU United Kingdom

- Bank Accounts – 44%
- Cryptocurrency Products – 30%
- Gaming Products – 19%
- Cash Products – 19%

Infographic: Key observations of reports resulting in dissemination to top 3 FIU counterparts.

2.4 Product Analysis

The analysis revealed that bank and e-money accounts were the most frequently utilised products identified within reports about OCGs, appearing in 51% of reports. Gaming products featured in 33% of reports, with activity typically carried out using table games and sports betting, with gaming machines featuring to a lesser extent. The use of cash and cryptocurrency products was also observed. This suggests a potential trend in which individuals with links to OCGs may attempt to launder illicit funds either via virtual assets or through cash-based vehicles to obscure the true origin of these funds[6].

6 The percentages do not add up to a 100% since multiple products may feature in a single report.

2.5 Red Flags Leading to Suspicion

The analysis indicated that, on average, each report concerning OCGs over the period of review contained approximately three triggers which prompted suspicions. Among these triggers, adverse media surrounding the subject of the report, as well transaction monitoring-based triggers featured to a prominent extent. The table below outlines the top five most frequently identified reasons for suspicion which led to the submission of reports concerning OCGs.

Commonly Identified Reasons for Suspicion
Unknown SOF/SOW
Concerns Surrounding Transactional Activity
Adverse Media
Uncooperative Customer
Suspected Beneficial Ownership Concealment

Table 5: Key Triggers Leading to Submission of Reports Relating to OCGs

A key trigger of suspicion relates to the source of funds/wealth of the involved persons and their overall transactional activities. Concerns about the source of funds/wealth are most frequently raised by Remote Gaming Operators, followed by credit and financial institutions.

In this context, it is important to note that adverse media screening plays a critical complimentary role, enabling reporting entities to further substantiate suspicions initially identified through transaction monitoring. The combined use of these data sources serves to strengthen the rationale for reporting by providing additional context on the potential criminal background of the individuals involved, thereby raisng additional concerns about the legitimacy of the source of wealth/funds utilised in such activity.

Additionally, reports received from the remote gaming sector most commonly note that the customer was uncooperative, often refusing to provide the requested documentation to verify the source of funds/wealth.

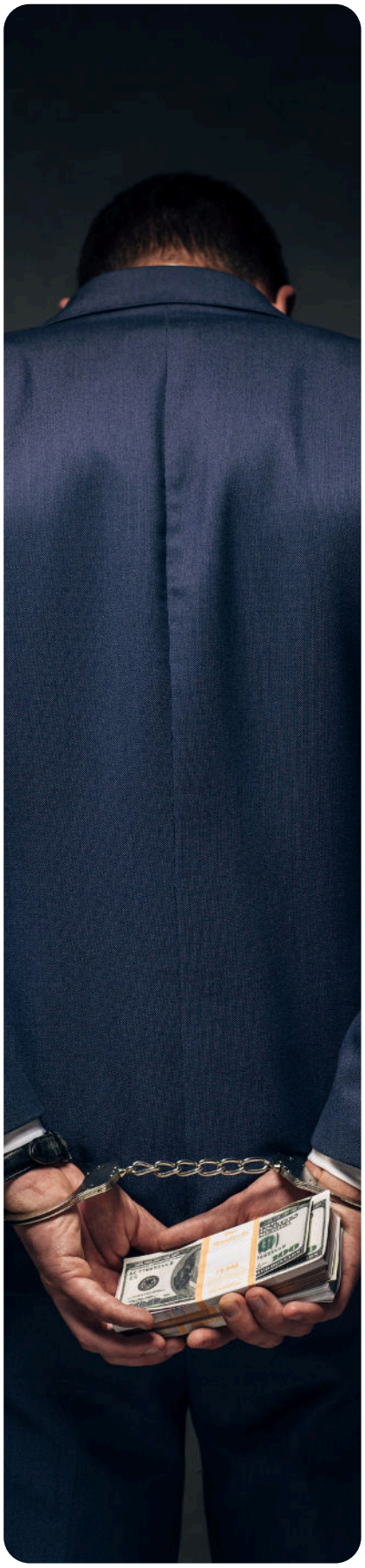
Furthermore, concerns about the transactional activity of the involved persons are most typically highlighted within reports submitted by credit and financial institutions. Concerns are typically raised about transactional activities that fall outside the customer's known profile, as well as transactions that are unnecessarily complex and have unclear narratives. This indicates that individuals involved in OCGs may be attempting to layer illicit funds through undertaking complex transactions to obscure the money trail.

2.6 Predicate Offences

2.6.1 General Overview

Overall, the analysis revealed that fraud was the leading predicate offence in reports linked to ML in relation to organised crime, appearing in 22% of all reports. It was identified that organised crime groups, both domestic and international, typically engage in various fraudulent activities, including card payment and online payment fraud, fraudulent investment schemes, identity theft and the use of forged documentation to launder money.

In line with the above observation, Europol released two publications in 2025 centring around the threats of organised crime, namely the "Internet Organised Crime Threat Assessment[7]" and the "EU Serious and Organised Crime Threat Assessment[8]". In both publications, fraud through identity theft is highlighted as a major concern, with criminals using stolen personal data to create fake identities. These stolen identities are then used to commit various types of financial fraud, including applying for bank accounts, subsidies and loans. These accounts are noted to then serve as mule accounts to receive and funnel criminal proceeds, further obscuring the source of the funds. Furthermore, artificial intelligence is highlighted as a catalyst for these crimes, enabling new forms of fraud, extortion and identity theft. Considering the prevailing threat of identity theft, the FIAU notes that only 1.5% of all reports received relating to OCGs involved elements of identity theft, indicating a potential under-detection of such fraudulent activities in connection with OCGs.



7 Source: Europol. (2025). Steal, deal and repeat: How cybercriminals trade and exploit your data (Internet Organised Crime Threat Assessment 2025). The percentages do not add up to a 100% since multiple reasons for suspicion may be chosen for a single report.

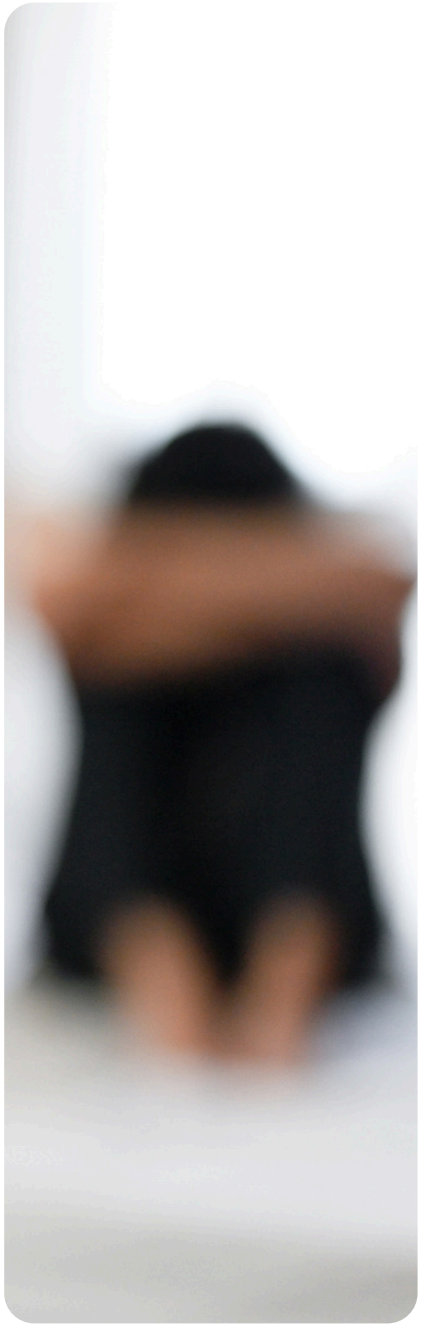
8 Source: Europol. (2025). The changing DNA of serious and organised crime: European Union Serious and Organised Crime Threat Assessment The percentages do not add up to a 100% since multiple reasons for suspicion may be chosen for a single report.

Additionally, the illicit trafficking in narcotic drugs and psychotropic substances featured in 20% of reports, further reaffirming its enduring role as a major source of illicit funds for OCGs.

Lastly, tax crimes are noted to have featured in 17% of reports, reflecting the prominence of tax evasion and similar related offences within the typical Modus Operandi of OCGs.

Through the strategic analysis on *'Maltese Massage Parlours and Their Possible Exposure to The Sexual Exploitation of Women,'* the FIAU also managed to identify links between organised crime groups and illicit massage businesses. In this publication[9], the FIAU explained that organised crime networks also tend to exert their influence over these illicit massage businesses. This is done by providing them with a variety of services, including facilitating connections and protection, thereby increasing the business's profitability. Such connections may include networks to recruit more victims, as well as channels to launder the illicitly gained funds.

The Illicit massage business might also form part of complex sexual exploitation networks. In fact, an array of clusters was identified, with multiple persons possibly forming part of organised criminal groups, who were found to have a direct or indirect connection with the massage establishment under analysis.



9 Source: Financial Intelligence Analysis Unit. (2024). Strategic Analysis on Maltese Massage Parlours and their Possible Exposure to the Sexual Exploitation of Women. https://fiaumalta.org/app/uploads/2024/05/Intelligence-Factsheet.pdf

2.6.2 International Organised Crime Groups

The analysis revealed that illicit trafficking in narcotic drugs and psychotropic substances was the suspected primary predicate offence in reports linked to ML relating to foreign organised crime, accounting for approximately 28% of cases. This predominance underscores the international nature of drug trafficking networks and their reliance on financial systems to launder proceeds of crime. For instance, the FATF publication "Money Laundering from Fentanyl and Synthetic Opioids" presents how international organised crime groups traffic synthetic opioids and launder the illicit funds by using the financial systems, primarily through money value transfer services (including hawala) or through correspondent banking arrangements[10].

Fraud followed closely at 23%, indicating a substantial overlap between organised crime and fraud schemes. A link to robbery and theft was found in 8% of the reports.

2.6.3 Domestic Organised Crime Groups

In reports linked to domestic organised crime groups, tax evasion was the leading suspected predicate offence, representing 40% of cases. Fraud accounted for 16%, further reinforcing its significance across both domestic and international contexts. Illicit trafficking in narcotic drugs and psychotropic substances accounted for 12% of reports, demonstrating that while less prevalent than tax evasion, it remains a notable component of domestic organised crime activities[11].

Furthermore, when considering reports involving both domestic and international organised crime groups, tax crimes were the leading suspected predicate offence, amounting to 33%. Fraud is noted to follow closely, with 31% of reports linked to suspected fraudulent activities. This indicates that money laundering through hybrid organised crime structures frequently utilises complex combinations of various predicate offences, inherently increasing the complexity of such criminal activity.

10 Source: Financial Action Task Force. (2022). Money Laundering from Fentanyl and Synthetic Opioids. The percentages do not add up to a 100% since multiple reasons for suspicion may be chosen for a single report.

11 The percentages do not add up to a 100% since multiple reasons for suspicion may be chosen for a single report.

2.7 Amounts Involved

The analysis highlights a clear distinction between international and domestic organised crime exposure in Malta. International organised crime reports generally indicate relatively low-value financial flows, with most cases involving suspected illicit funds in the range of €0 to €10,000. In contrast, domestic organised crime reports consistently reflect significantly higher monetary exposure, with a substantial proportion of cases involving amounts between €100,001 and €500,000.

This disparity suggests that international cases linked to Malta are more likely to reflect transactional or intermediary activity with a limited financial footprint, whereas domestic organised crime appears to generate and retain more substantial proceeds within the local jurisdiction, resulting in higher-value laundering activity being captured in intelligence reporting.

Conclusion

This analysis of organised crime reports processed by the FIAU between 2021 and 2024 provides a comprehensive overview of the landscape of illicit organised criminal groups linked to Malta. The data revealed distinct patterns in both domestic and international organised crime, highlighting the varying exposures and reporting capabilities of different sectors. It is noteworthy that remote gaming operators play a significant role in identifying threats from both international and national OCGs, which are not necessarily operating within Maltese borders. Similarly, credit institutions appear to demonstrate a strong capacity to detect illicit activities featuring elements of both domestic and international organised crime. The predominance of multiple suspected predicate offences within the same report, coupled with the frequent use of various suspicion indicators, underscores the complexity and evolving nature of organised criminal groups.

Subject persons are encouraged to maintain a comprehensive and risk-sensitive approach when monitoring customer activity involving cross-border transactions, particularly where such activity involves jurisdictions with which there is a higher volume of financial interaction.

In this regard, attention should be given to ensuring that transaction monitoring frameworks and customer due diligence measures adequately capture activity conducted through a range of financial products, including banking services, electronic money instruments, and gaming-related services. These controls should be proportionate and capable of identifying patterns of activity that may warrant further review.

Operators within the remote gaming sector are similarly reminded of the importance of maintaining effective monitoring mechanisms for cross-border transactions. This includes ensuring that systems are sufficiently robust to identify unusual or inconsistent activity that may arise in an international context, taking into account the nature of the products and services offered.

Furthermore, subject persons dealing with virtual financial assets or related services should ensure that appropriate safeguards are in place to support the transparent and traceable use of such instruments. This includes maintaining adequate oversight of transactional behaviour and ensuring alignment with applicable AML/CFT obligations.

Overall, subject persons should adopt a holistic approach to risk management by ensuring that internal controls, monitoring systems, and reporting practices remain responsive to evolving transactional patterns and continue to support the timely identification and reporting of potentially suspicious activity.

Subject persons are requested to quote the code “SA26-1” when submitting reports arising from this publication.

Questions on this document may be sent to:
strategicanalysis@fiaumalta.org

Financial Intelligence Analysis Unit
Trident Park, No. 5, Triq l-Mdina,
Central Business District Birkirkara, CBD 2010

Telephone: (+356) 21 231 333
E-mail: info@fiaumalta.org
Website: www.fiaumalta.org