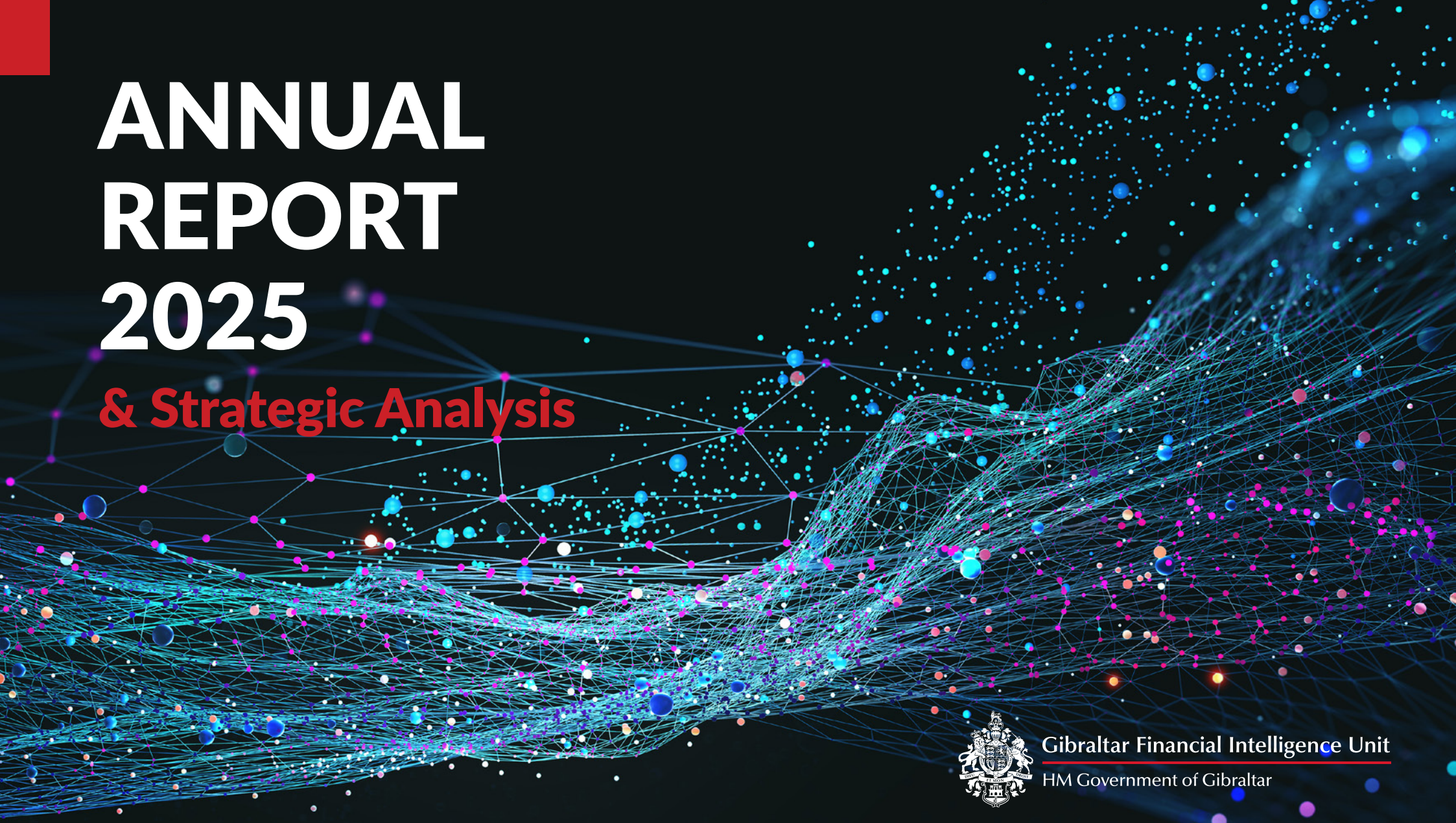
ANNUAL REPORT 2025

& Strategic Analysis



Gibraltar Financial Intelligence Unit

HM Government of Gibraltar

TABLE OF CONTENTS

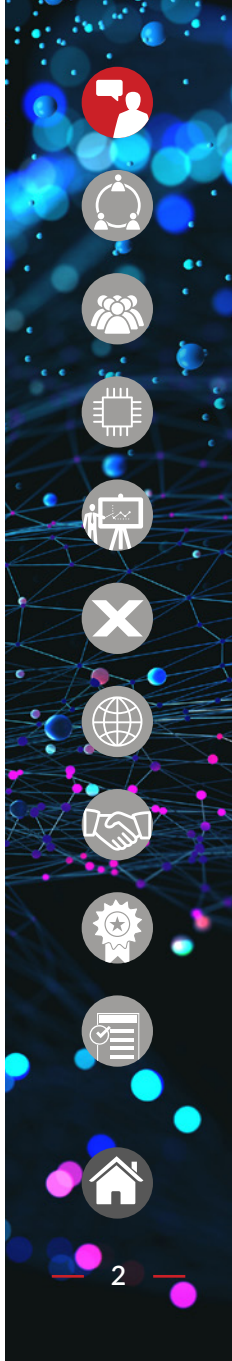
Your Feedback Matters

Your feedback is invaluable in helping us improve the quality and relevance of our analysis. Whether you have suggestions for improvement, questions, or comments, we welcome all input.

To share your thoughts, please

Click Here

Your feedback will be carefully considered and used to enhance future versions of this document.



Edgar lopez
Director, GFIU

It is my pleasure to present the Gibraltar Financial Intelligence Unit's (GFIU) Annual Report and Strategic Analysis for 2025, setting out the work and developments of the Unit during the reporting period. This report also marks my final year as Director of the GFIU as I step down from the role.

The operating environment continues to evolve at pace. Financial crime is increasingly complex, transnational and technology-enabled. Traditional typologies persist, but are now accompanied by more sophisticated methods, including the use of virtual assets, online platforms and decentralised financial networks. At the same time, broader geopolitical developments, sanctions regimes and emerging risks are reshaping the context in which financial intelligence is produced and applied. These dynamics reinforce a central point, that financial intelligence is no longer confined to supporting investigations alone, it is integral to understanding and responding to wider national security threats.

These developments have contributed to a sustained increase in demand for financial intelligence. In 2025, the GFIU received 5,000 suspicious activity reports, the highest level recorded to date. This increase reflects a more engaged reporting sector and a system that is becoming progressively more responsive to risk. However, volume alone is not a measure of effectiveness. The more significant development has been in the quality and relevance of reporting. Through outreach, feedback and targeted engagement, under Project Nexus and e-Nexus, the standard of reporting has improved, supporting more focused and actionable analysis.

As volumes increase, so too do the demands on prioritisation, analytical capacity and data management. In response, the GFIU has continued to strengthen its internal capabilities. The development of integrated solutions to support workflow management and data governance has enhanced our ability to manage complexity while maintaining analytical consistency. The application of the National Decision Model across all areas of work has further embedded a structured, risk-based approach, ensuring that decisions are aligned to operational priorities.

Complementing its operational work, the GFIU has enhanced its strategic intelligence capability. The introduction of internal Fintel Briefs has enabled us to provide timely assessments of emerging threats. These are designed to support stakeholders in better understanding the convergence between financial crime and national security risks, including sanctions evasion, proliferation financing and the financial dimensions of geopolitical developments. This reflects an increasing recognition of financial intelligence as both an operational enabler and a strategic capability within the wider framework.

Cooperation remains fundamental. Internationally, the importance of timely and effective information exchange continues to grow. At the domestic level, the Joint Financial Intelligence Tasking Group continues to provide a mechanism for multi-agency coordination, ensuring that intelligence is considered early and directed towards appropriate outcomes. Engagement with the private sector has also strengthened, contributing to improved reporting quality and a more consistent understanding of risk across sectors.

The reporting period has also been shaped by the need to align with the current evaluation cycle of the FATF which places an increased emphasis on effectiveness. This is of particular relevance in the context of Gibraltar's forthcoming MONEYVAL assessment in 2027, where the GFIU will be a key contributor to that assessment.

Looking ahead, the challenge is not only to keep pace with a changing threat landscape, but to anticipate it. This requires continued investment in capability, sustained partnership across the public and private sectors and a clear focus on outcomes.

None of the progress set out in this report would have been possible without the professionalism and dedication of GFIU staff and the continued support of our partners across government, law enforcement, supervisory authorities and the private sector.

It has been a privilege to lead the GFIU during a period of significant development. The Unit is well placed to build on these foundations and continue strengthening its contribution to Gibraltar's response to financial crime.

This report sets out the detail behind that progress and the basis for what comes next.

OUR ORGANISATION

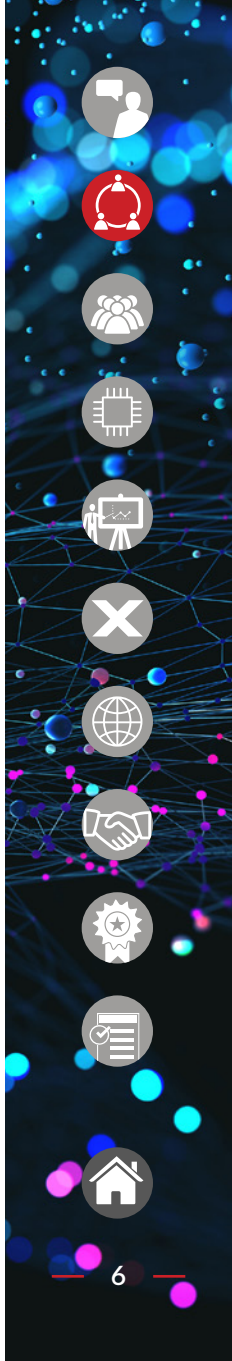
The Gibraltar Financial Intelligence Unit (GFIU) serves as Gibraltar's central hub for financial intelligence. Established in January 1996, its core mandate is to collect, store, analyse, and disseminate intelligence linked to criminal activities, including money laundering, terrorism financing, and the proliferation of weapons of mass destruction.

As a key player in combating financial crime, the GFIU leads and participates in several working groups, including the Joint Financial Intelligence Tasking Group, the Joint Coordinating Intelligence Group to Counter Proliferation Financing, and the Financial Liaison and Intelligence Network (FLINT).

Through its outreach initiative, Project Nexus, the GFIU provides essential guidance to financial institutions, increasing awareness of money laundering, terrorist financing, human trafficking, and proliferation threats. It also offers specialized guidance to reporting entities, improving the quality of Suspicious Activity Reports (SARs).

The GFIU operates under the leadership of a Director and is composed of Domestic, International, and Analysis Desks, supported by Intelligence Managers, Financial Intelligence Officers, International Liaison Officers and Analysts The team also includes seconded specialists from the Royal Gibraltar Police, HM Customs, the Income Tax Office and the Gambling Division. Oversight of operations is managed by the Head of Operations, who also provides internal legal support. The GFIU adheres to Financial Action Task Force (FATF) recommendations and is evaluated by MONEYVAL, the Council of Europe's committee for assessing AML and CFT measures.

The GFIU is a member of the Egmont Group of Financial Intelligence Units, an associate member of the International Anti-Corruption Coordination Centre (IACCC), and an active participant in Europol's Financial Intelligence Public-Private Partnerships (EFIPPP). Additionally, the GFIU collaborates with Cifas, the UK's fraud prevention database, and partners with the Royal United Services Institute (RUSI), strengthening its role in the global fight against economic crime. It is also a member of the Quad Forum, alongside FIUs from Guernsey, the Isle of Man, and Jersey.




OUR PEOPLE

Director

Edgar Lopez began his career with the Royal Gibraltar Police, serving predominantly within specialist units of the Crime and Protective Services Division. He went on to hold leadership roles, including Head of Special Branch, Head of the Interpol Gibraltar Sub-Bureau, and GFIU's Head of Projects, where he developed expertise in intelligence, counter-terrorism, and international intelligence exchange.

He holds a Master's degree in International Affairs with a specialisation in Cybersecurity from King's College London. His academic research focused on the use of the cyber domain by state actors to finance illicit nuclear weapons and missile programmes, reflecting an early and sustained engagement with proliferation financing.

As Director of the GFIU, Edgar has led the unit through a period of significant development, strengthening its operational capability, governance, and international standing. He has extensive experience of the Financial Action Task Force and MONEYVAL processes.

Internationally, Edgar is recognised as a practitioner and adviser in counter-proliferation financing. He has provided technical assistance and specialist guidance to other jurisdictions on developing proliferation financing risk assessments, strengthening operational frameworks, and establishing effective public-private partnerships. Through this work, he has supported enhanced international cooperation and strengthened Gibraltar's continued engagement as a trusted and respected participant.

Head of Operations

Carl Ramagge joined the Gibraltar Financial Intelligence Unit as Head of Operations in December 2021. He was called to the Bar of England and Wales, and Gibraltar, in 2007 and brings almost twenty years of experience across criminal justice, prosecution, and financial crime.

In 2013, Carl was appointed Crown Counsel for HM Government of Gibraltar, where he spent eight years at the Office of Criminal Prosecutions and Litigation (OCPL). During this period, he was involved in some of Gibraltar's most significant and complex criminal proceedings, including cases of murder, rape, serious sexual offences, and offences involving children. He also completed specialist training in Rape and Serious Sexual Offences with the Crown Prosecution Service in the United Kingdom.

Carl's prosecutorial experience extends to economic crime, including fraud and false accounting, with a number of cases resulting in the successful confiscation of criminal proceeds. This background has provided a strong foundation for his role at the GFIU, where proportionality and integrity are central to operational decision-making.

As Head of Operations, Carl provides operational oversight and internal legal governance across the Unit, supporting intelligence-led activity that is outcome-focused. He has continued to develop specialist expertise in financial intelligence, sanctions, and economic crime, including the commencement of a global sanctions specialist course.

Internationally, Carl's expertise has been recognised through his selection as Chair of the Policy and Procedures Working Group of the Egmont Group of Financial Intelligence Units. In this role, he co-leads on a project focused on Operational Independence and contributes to the development of operational standards, guidance, and best practice that support effective and secure information exchange between FIUs worldwide.

Carl remains actively engaged in outreach and partnership activity, playing a key role in Project Nexus and regularly delivering at engagement clinics and industry events. His leadership continues to strengthen the GFIU's operational resilience, international standing, and engagement with both domestic and global partners.

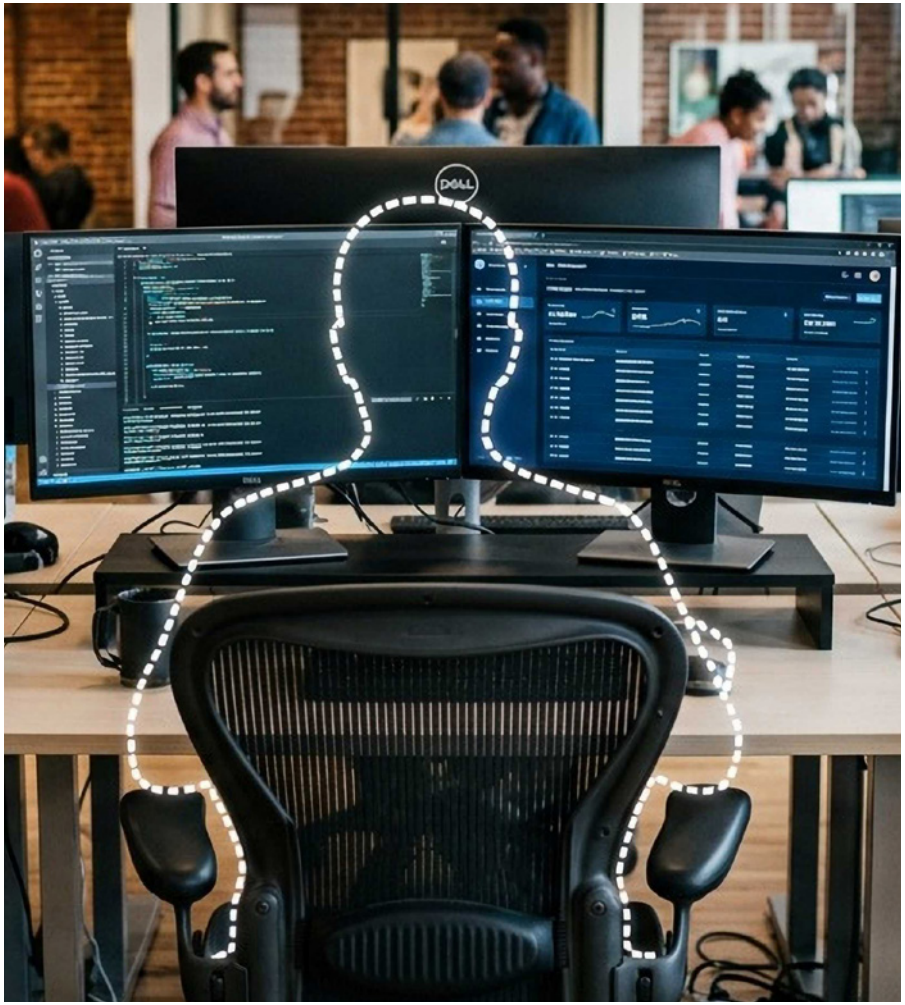
Note: At the time of publishing, Carl has since been appointed as Director of the GFIU.

Our team

The GFIU's operational framework, structured around International, Domestic, and Analysis Desks, enables a responsive and adaptable approach to financial intelligence. The Analysis Desk plays a central role in supporting the wider organisation, working closely with Financial Intelligence Officers (FIOs) and Financial Intelligence Support Officers to deliver high-quality intelligence products. This collaborative, multi-disciplinary model supports a modern working environment and strengthens the GFIU's ability to meet its operational objectives.

The GFIU places a strong emphasis on inclusivity and diversity, recognising that a broad range of skills, experience, and perspectives enhances analytical judgement, decision-making, and problem-solving. Staff are supported to develop professionally and to contribute fully to the Unit's performance through structured mentoring, in-house training, and continuous development opportunities. All officers complete internal training programmes, followed by accredited Financial Intelligence Officer training delivered by the UK's Proceeds of Crime Centre, the body responsible for accrediting and overseeing financial investigators in England, Wales, and Northern Ireland.

A positive and supportive organisational culture underpins the GFIU's effectiveness. Leadership and management practices promote accountability, empowerment, and innovation, and are aligned with the GFIU's three-year Strategic Plan. Training remains a core component of the GFIU's mandate, ensuring that core skills are maintained and developed in line with emerging risks. This is supported through regular in-house sessions and access to external e-learning platforms, including the Egmont Group's ECOFEL programme, enabling staff to remain informed and effective in a continually evolving threat environment.




OUR TECHNOLOGY

Technology underpins the GFIU's ability to manage complexity, safeguard sensitive information, and deliver high-quality financial intelligence in an increasingly data-rich and fast-moving environment. In recent years, the GFIU has invested significantly in the development of tecnology and in-house systems designed to support the full financial intelligence lifecycle, from the receipt of data and tasking through to analysis, dissemination, and review.

At the centre of this architecture is THEMIS an integrated case and intelligence management system that enables the secure receipt, storage, and handling of Suspicious Activity Reports (SARs) and associated intelligence. Built using a modular design, the system is engineered to be resilient and interoperable, allowing functionality to evolve in line with operational demand and emerging risk.

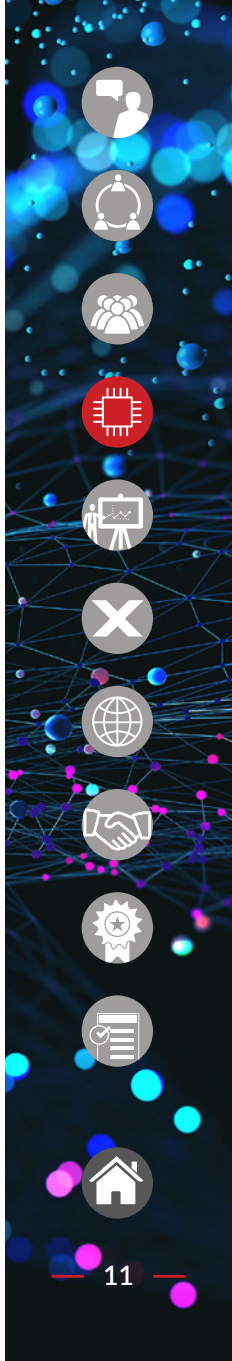
During the reporting period, the platform underwent a user interface and user experience redesign, informed by user needs.

THEMIS supports structured and unstructured data collection, enabling detailed reporting while retaining flexibility where information is limited or develops over time. Secure, role-based access controls allow the GFIU, law enforcement agencies, and the Government Law Offices to engage with the system in a controlled and auditable manner. Embedded communication tools facilitate the secure exchange of information, follow-up enquiries, and the dissemination of intelligence reports, ensuring strong governance and compliance with legal and information-handling requirements.

Beyond SAR management, the system functions as a centralised intelligence repository, consolidating international intelligence exchanges, spontaneous disclosures, MLA requests, law enforcement notifications, and analytical outputs. Enhanced workflow management and task-tracking capabilities provide an accurate oversight of operational activity, supporting prioritisation, accountability, and outcome monitoring.

Advanced data visualisation and dashboarding tools enable analysts and managers to interrogate trends, identify emerging risks, and assess reporting patterns at both sectoral and jurisdictional levels. These capabilities provide critical insights for both operational and strategic intelligence activity.

In parallel, the GFIU continues to deploy specialist analytical technologies to address emerging financial crime threats. This includes the use of advanced blockchain analytics tools to trace transactions across public distributed ledgers, identify clustering behaviour, and detect links to known threat actors. These tools allow Financial Intelligence Officers to follow complex transactions across wallets, exchanges, and jurisdictions, supporting the identification of proceeds of crime and timely intervention by law enforcement.



Open Source Intelligence (OSINT) capabilities are fully integrated into the analytical workflow, allowing Financial Intelligence Officers to enhance financial intelligence through publicly available information from media sources, corporate registries, social media platforms and online databases. OSINT provides contextual depth, supports network analysis, and reveals behavioural patterns or associations that may not be immediately apparent through financial data alone.

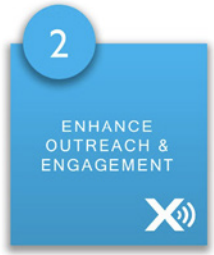
The GFIU continues to explore the responsible application of advanced technologies, including artificial intelligence, to enhance pattern recognition, anomaly detection, and analytical efficiency. These developments are pursued with a clear focus on governance, transparency, and professional judgement, ensuring that technology acts as an enabler of effective intelligence rather than a substitute for human expertise. In order to manage the complexities of the use of AI, the GFIU introduced a policy that establishes guidelines for the responsible and secure use of AI solutions. It ensures that AI tools are used ethically and in compliance with data protection laws, preventing unauthorised disclosure of sensitive financial intelligence.


OUR STRATEGY

The 2023-2026 Strategic Plan continues to guide the GFIU's role in countering financial crime. Built on the four "E's"— Elevate, Enhance, Expand, and Embrace—this strategy sharpens the GFIU's focus on operational priorities while advancing staff development, innovation, and collaboration with stakeholders.

Elevate Resource Capacity

Demonstrates our intent to build on progress already made and equip our people with the skills they need to excel. The GFIU is committed to working with our partners to incorporate new means of learning and collaboration. Developing the quality and quantity of intelligence reports produced is a key goal.



Enhance Outreach and Engagement

Demonstrates our commitment to our flagship outreach initiative, Project Nexus, which was launched in 2017. Improving our delivery and content is an ongoing aim. Engaging with the private sector builds mutual understanding, facilitating greater knowledge of stakeholders' needs and responsibilities. Our e-Nexus platform provides online courses, which encourages active learning and allows users to tailor their training to their needs and schedule.

Expand Partnership and Collaboration

Demonstrates our continued engagement with local and international partners in the fight against financial crime. We are always on the lookout to expand our network, ensuring we remain at the forefront of developments

Embrace Innovation and Technology

Demonstrates our desire to harness technology through the acquisition of new analytical tools and information sharing systems. As cyber-enabled financial crime continues to rise, so does our need to stay one step ahead. The GFIU is committed to using technology to address emerging threats effectively. Digital transformation remains at the heart of its strategy, ensuring enhanced intelligence capabilities and a more resilient approach to financial crime prevention.

OUR OUTREACH – PROJECT NEXUS

PROJECTNEXUS

Project Nexus is the GFIU's flagship outreach and engagement programme, designed to strengthen collaboration between the public and private sectors in the fight against financial crime. The initiative is built on the principle that effective financial intelligence depends on strong, informed, and trusted relationships between reporting entities, regulators, and law enforcement.

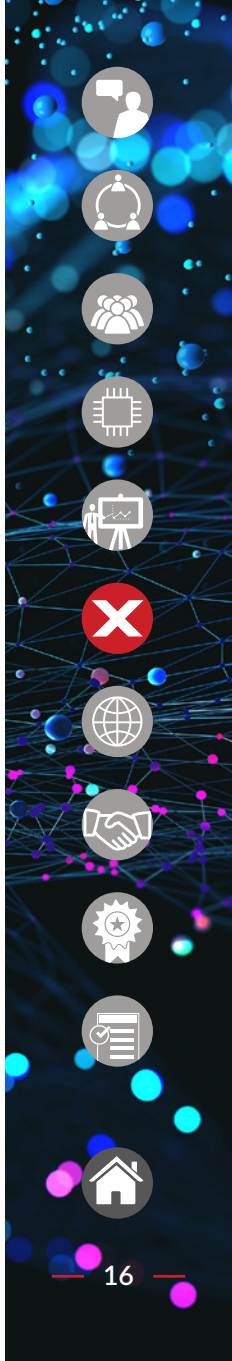
During 2025, Project Nexus experienced significant demand from the private sector, reflecting a growing appetite for practical guidance, dialogue, and shared understanding of financial crime risk. In response, the GFIU undertook a targeted review of its outreach delivery model to ensure that engagement activity remained relevant, effective and aligned with the operational needs faced by reporting entities.

As a result, the Project Nexus programme was redesigned to place greater emphasis on practical, scenario-based exercises and applied learning, moving beyond traditional presentation-led formats. Engagement sessions and clinics were structured around case studies, typologies, indicators, and decision-making challenges, allowing participants to apply legislative and regulatory requirements in a controlled, interactive environment. This approach was particularly well received and has contributed to a clearer and more consistent understanding of financial crime risks, reporting thresholds, and intelligence value across participating sectors.

The continued delivery of Project Nexus Engagement Clinics has played a central role in this evolution. These clinics provide targeted, sector-specific training that supports professionals in identifying suspicious activity, articulating suspicion clearly, and submitting higher-quality Suspicious Activity Reports (SARs). Feedback and post-engagement analysis indicate measurable improvements in both the quality and usefulness of SARs submitted following participation in these sessions.

Project Nexus delivery is aligned with the GFIU's wider corporate communications and engagement strategy and makes use of multiple channels to maximise reach and accessibility. Participant feedback throughout the year has remained consistently positive, with engagement activity widely regarded as relevant, practical, and directly applicable to day-to-day compliance and risk management functions.

Through Project Nexus, the GFIU continues to strengthen the quality of financial intelligence at source, enhance mutual understanding of risk, and support a more effective, intelligence-led response to financial crime across Gibraltar.



e-Nexus series

The e-Nexus Series is the GFIU's digital learning platform, developed to support continuous awareness and capability-building among financial and non-financial reporting entities. The platform complements in-person engagement by providing structured, on-demand access to learning resources that reflect current risks, regulatory expectations, and international standards.

e-Nexus delivers interactive workshops and modular training covering a range of topics, including legislative and regulatory updates, emerging financial crime typologies, and international AML/CFT/CPF obligations. Content is designed to be practical and scenario-led, supporting the application of knowledge to real-world compliance and reporting challenges.

With a growing user base of over 1700 users, the platform enables flexible engagement, allowing professionals to access relevant material at a pace and time that suits operational demands. User feedback throughout the year has been consistently positive.

Through e-Nexus, the GFIU continues to extend the reach of its outreach programme, reinforce key messages delivered through Project Nexus, and support sustained improvements in understanding and effectiveness across reporting sectors. In parallel, a growing number of jurisdictions are engaging with the GFIU to better understand the e-Nexus model and its effectiveness as a structured approach to training reporting entities.


OUR INTERNATIONAL WORK

EGMONT GROUP
OF FINANCIAL INTELLIGENCE UNITS

The Egmont Group of Financial Intelligence Units facilitates and promotes the exchange of information, knowledge, and cooperation between member Financial Intelligence Units in their shared efforts to combat financial crime. A member since 2004, the GFIU actively exchanges intelligence with international counterparts and continues to contribute to Egmont's operational and strategic work.

In 2025, the GFIU participated in the Egmont Working and Regional Group virtual meetings and attended the 30th Egmont Plenary in Luxembourg. These forums support effective global collaboration and ensure that the GFIU remains at the forefront of international financial intelligence-sharing.

In addition, the Head of Operations, Carl Ramage, was selected as Vice Chair of the Policy and Procedures Working Group, where he has played a leading role in advancing a high-level project examining FIU operational independence.

As part of the Europe II Group, the GFIU acted as a co-lead on a project undertaking a horizontal review of Financial Action Task Force Immediate Outcomes 2 and 6, and Recommendations 29 and 40. The project has since been finalised and published, producing a valuable reference document that supports the effective implementation of international standards across FIUs.

IACCC
International Anti-Corruption Coordination Centre

The GFIU became an Associate Member of the International Anti-Corruption Coordination Centre (IACCC) in 2020, strengthening its ability to support complex international corruption investigations. Hosted by the National Crime Agency in London, the IACCC enables Financial Intelligence Units and law enforcement agencies, particularly those from smaller financial centres, to rapidly exchange intelligence and contribute to the development of comprehensive intelligence pictures in cases of grand corruption.

Comprised of nine law enforcement agencies from Australia, Canada, New Zealand, the United Kingdom, the United States, and Singapore, the IACCC provides specialist support to partners worldwide, including assistance with the coordination and facilitation of Mutual Legal Assistance (MLA) requests. Through a dedicated liaison officer, the GFIU actively facilitates intelligence-sharing on grand corruption matters and benefits from specialist training in areas such as bribery, cryptocurrency investigations, and open-source intelligence.

In 2025, the GFIU attended an IACCC partners' meeting hosted in Guernsey, which brought together key stakeholders to examine emerging threats at the intersection of grand corruption and increasingly sophisticated financial and cyber-enabled crime. The meeting provided an important forum to strengthen international partnerships, exchange best practices, and consider innovative approaches to enhancing the global response to corruption. Participation in this forum further reinforced the GFIU's commitment to active international cooperation and continued engagement in initiatives focused on training, guidance, and operational effectiveness.

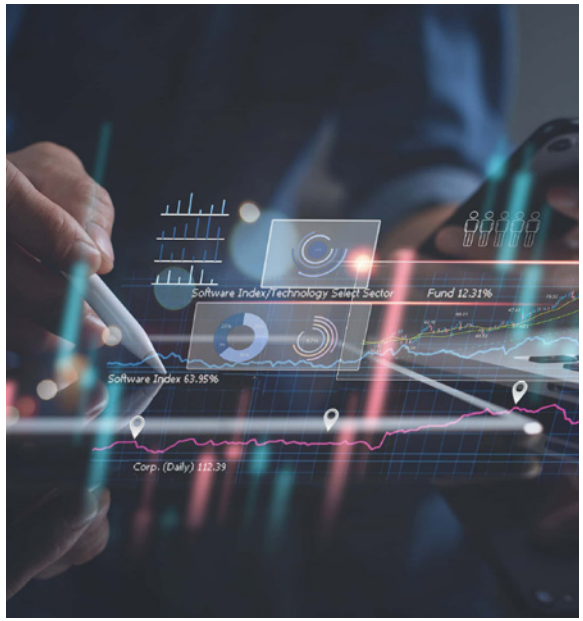
QUADFORUM
Strategic Collective of Financial Intelligence Units

The GFIU collaborates closely with counterpart Financial Intelligence Units from Guernsey, Isle of Man, and Jersey through the Quad Forum. This partnership provides a structured platform for the sharing of best practice, joint training, and enhanced cooperation with law enforcement agencies across comparable international finance centres.

In 2025, the Quad Forum facilitated a specialist course on terrorist financing delivered in collaboration with the National Terrorist Financing Intelligence Unit, further strengthening collective capability and operational understanding in this critical risk area. The Forum also met regularly with Economic Crime Units to discuss emerging threats, trends, and typologies across member jurisdictions. These engagements supported shared awareness and operational preparedness, while also providing a forum to exchange best practice and experience in preparation for forthcoming MONEYVAL assessments.

Throughout the year, the Quad Forum also continued its work on a comparative analysis examining the commonalities and differences across member jurisdictions. This exercise has deepened mutual understanding of each jurisdiction's operational context while reinforcing a shared strategic identity. By identifying areas of alignment and divergence, the analysis is helping to shape the future direction of the Quad Forum and provides a strong foundation for coordinated responses to evolving financial crime threats.

Rooted in a shared commitment to international cooperation and underpinned by similar values, structures, and challenges, this collaborative work enhances the collective ability of Quad Forum members to mitigate transnational crime and positions the Forum as a strong and effective partnership in the global fight against financial crime.




OUR PARTNERSHIPS

CFCS RUSI Centre for Financial Crime & Security Studies

Since 2023, the GFIU has been partnered with the Centre for Finance and Security at the Royal United Services Institute (RUSI), a leading security and defence think tank based in Whitehall, London. Established in 2014, the Centre for Finance and Security focuses on strengthening resilience in the global response to illicit finance, challenging conventional approaches, and producing influential research and policy analysis.

This collaboration has enhanced the GFIU's engagement in research, policy development, and capacity-building initiatives aimed at preventing financial crime and strengthening international frameworks.

During 2025, the GFIU participated in a number of conferences and initiatives hosted by RUSI, including the Maritime Sanctions Taskforce and the UK Sanctions Implementation and Strategy Taskforce. Participation in these forums ensured that the GFIU remained actively engaged in key international discussions on financial crime, sanctions, and security, and was able to contribute practical financial intelligence perspectives to evolving policy debates.

United For Wildlife

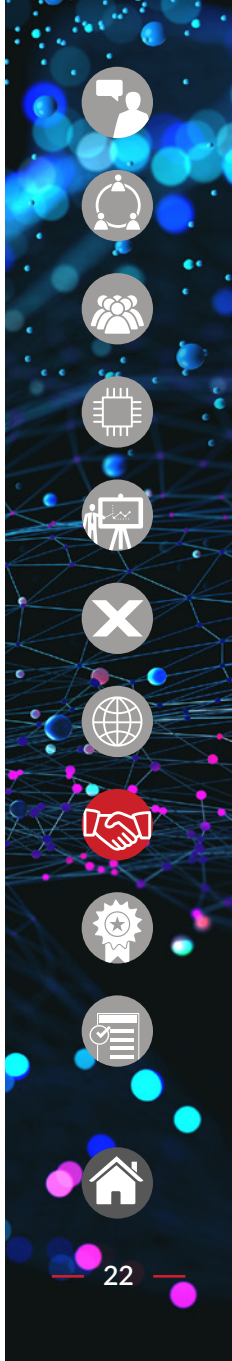
In 2025, the GFIU signed a Statement of Principles with United for Wildlife, formalising a commitment to a coordinated approach to combating the illegal wildlife trade. The Statement set out a framework for cooperation focused on the effective use of financial intelligence, enforcement capability, legal frameworks, and awareness-raising to disrupt the financial and operational networks that underpin this form of serious and organised crime.

Established in 2013 by Prince William through The Royal Foundation of The Prince and Princess of Wales, United for Wildlife brings together financial institutions, transport and logistics providers, conservation organisations, and law enforcement agencies. Its objective is to prevent criminals from transporting, financing, or profiting from illegal wildlife products and to disrupt a transnational crime that continues to place significant pressure on vulnerable species worldwide.

Through its Financial Taskforce, Transport Taskforce, and Regional Chapters, United for Wildlife has promoted cross-sector collaboration and intelligence-led action, recognising that illicit financial flows are a critical enabler of wildlife trafficking and associated criminal activity.

The GFIU has long recognised that the illegal wildlife trade is not solely an environmental concern, but one that is closely linked to organised crime, corruption, and illicit financial flows. This risk is identified in Gibraltar's 2025 National Risk Assessment, which highlights the potential for misuse of international financial systems and Gibraltar's strategic position as a financial centre in facilitating or obscuring the proceeds of wildlife-related crime.

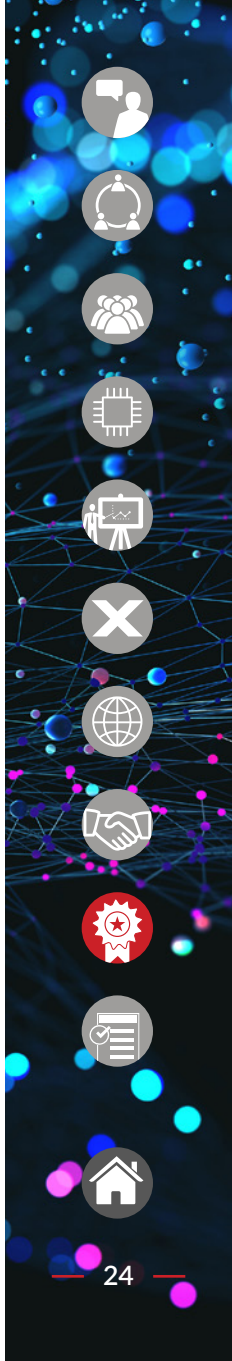
By joining this initiative, the GFIU strengthened its contribution to international efforts to identify, disrupt, and dismantle the financial networks associated with wildlife trafficking. Engagement with United for Wildlife partners enhanced intelligence-sharing and reinforced the role of financial intelligence in breaking the financial chains that sustain the illegal wildlife trade.




OUR ACHIEVEMENTS

During 2025, the GFIU made further progress in strengthening its operational effectiveness, expanding international cooperation, and reinforcing engagement with public and private sector partners. These achievements demonstrate the Unit's proactive approach and continued focus on combating financial crime across all threat areas.

- Attended Seize: London 2025 at the United States Embassy in London, in collaboration with Asset Reality, a leading forum addressing emerging challenges in asset recovery.
- Hosted a bilateral meeting with the Financial Intelligence Unit of Moldova, supported by the OSCE, to exchange practical insights on financial analysis, tracing, and the freezing of crypto-assets.
- In collaboration with the Gibraltar Association of Compliance Officers (GACO), hosted a workshop titled "Unmasking the Financial Flows Behind Human Trafficking", delivered by subject-matter expert Mr Steve Farrer.
- Launched a completely redesigned GFIU website, introducing a modern, minimalist layout with enhanced usability and seamless performance across all devices.
- Published the GFIU's Corporate Communication Strategy 2025–2028, establishing a structured framework to strengthen engagement with key stakeholders, the private sector, public sector, the general public, and international counterparts.
- Attended a Europol Financial Intelligence Public-Private Partnership (EFIPPP) plenary meeting in Brussels, contributing to discussions on underground banking and emerging financial crime typologies.
- Released two new e-learning workshops on the e-Nexus platform, including interactive modules on ransomware—one of the most significant current threats—and understanding politically exposed persons.
- Hosted the Small States and Territories Working Group in Gibraltar, bringing together professionals and subject-matter experts to develop guidance on national risk assessments for proliferation financing and terrorist financing.
- Co-led a project examining proliferation financing risks in small states and territories, contributing to the development of practical guidance to support national risk assessment processes.
- Attended the tenth anniversary of RUSI's Centre for Financial Crime and participated in the Partnership Forum Ideas Lab.
- Contributed to discussions within RUSI's UK Maritime Sanctions Taskforce.
- Hosted Kharon to deliver sanctions-focused training to public and private sector stakeholders in Gibraltar, addressing the complexity of modern sanctions regimes.
- Facilitated sanctions-related training delivered by RUSI experts to key public sector stakeholders.



- Participated in a sanctions-focused tabletop exercise delivered by Sanctions SOS and hosted by the Ministry of Justice.
- Attended meetings and discussions in Miami focused on demonstrating FATF effectiveness in relation to sanctions, hosted by the UK Foreign, Commonwealth and Development Office (FCDO).
- Participated in the 3rd Crypto Symposium in Zug, Switzerland, organised by MROS and the Swiss Federal Police (Fedpol).
- Attended an INTERPOL workshop in North Macedonia focused on the operational use of the “Silver Notice” tool for the recovery of criminally acquired property.
- Attended a Virtual Asset Service Providers (VASPs) Risk-Based Supervision Training Symposium in Malta, hosted by the Financial Intelligence Analysis Unit (FIAU) Malta.
- Participated in the Global FIU Leadership Conference hosted by Egmont Centre for FIU Excellence and Leadership(ECOFEL) and FIU Switzerland (MROS), representing the largest FIU leadership gathering outside the Egmont Group Plenary meetings.


identity
STRATEGIC ANALYSIS REPORT

Strategic Analysis Overview

The Gibraltar Financial Intelligence Unit continues to strengthen and recalibrate its strategic analysis function to ensure that financial intelligence is translated into operational and policy outcomes. In recent years, a series of targeted initiatives have been implemented to enhance analytical quality, consistency, and practical utility. These measures have included the use of stakeholder surveys and internal review mechanisms to assess the effectiveness and impact of strategic outputs.

This report reflects an evolved analytical model, integrating financial intelligence within a structured strategic assessment framework. It provides a forward-looking evaluation of money laundering (ML), terrorist financing (TF), and proliferation financing (PF) risks affecting Gibraltar. The objective is to equip competent authorities, supervisory bodies, policymakers, and reporting entities with a clearer understanding of threat dynamics, systemic vulnerabilities, and emerging typologies within the jurisdiction's financial architecture.

The analysis is derived from multi-source intelligence and applies both quantitative trend assessment and qualitative risk evaluation. In particular, the report seeks to:

- Collate and interrogate annual SAR data to identify recurring patterns, typologies, and sectoral risk concentrations.
- Collect, assess, and integrate supplementary intelligence from domestic partners and other competent authorities to strengthen contextual interpretation.
- Identify linkages across datasets in order to uncover concealed relationships, cross-sector exposure, and areas of threat convergence.

The strategic findings presented highlight key money laundering threats and structural vulnerabilities, drawing primarily on Suspicious Activity Reports (SARs) submitted by Gibraltar-based reporting entities and supported by additional intelligence sources.

Following a review of prior statistical publications, the GFIU has refined its methodological approach. The scope of analysis is now limited to reports filed pursuant to the Proceeds of Crime Act 2015 and the Terrorism Act 2019. This recalibration enhances analytical coherence, strengthens year-on-year comparability, and ensures closer alignment with typologies and trends relating to ML, TF, PF, and associated predicate offences.

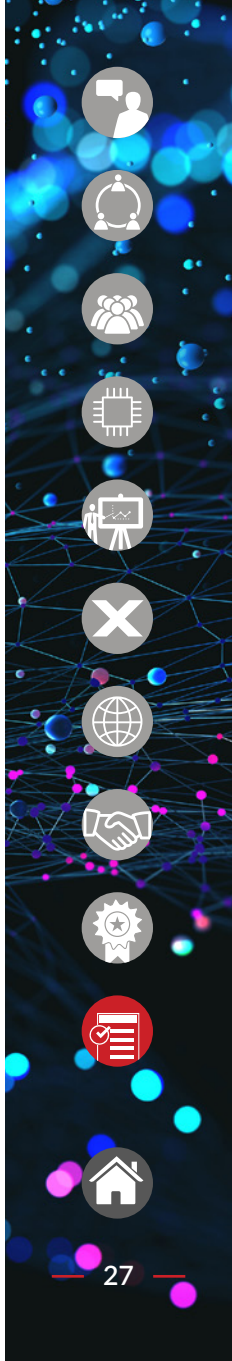
In 2025, the GFIU received 5,816 SARs, representing a 17.49% increase compared to 2024. Reporting remained concentrated, with the top ten reporting entities accounting for 77% of total submissions. The gaming sector remained the largest contributor, submitting 3,399 SARs (58% of the total), reflecting an 18% year-on-year increase.

90% of gaming sector SARs were also dual-reported to foreign jurisdictions, underscoring the cross-border dimension of associated risks. The banking sector recorded a significant 217% increase in reporting volumes, becoming the second-largest contributor and accounting for 19% of total SARs. By contrast, the Virtual Asset Service Provider (VASP) sector experienced a 45% decline in reporting during the same period.

A total of 99 reporting entities across 16 sectors submitted SARs in 2025, compared to 80 entities in 2024, indicating broader engagement across the regulated community and improved reporting outreach.

ML and fraud remained the most frequently reported suspected criminal activities. A marked increase in payment-related and cyber-enabled fraud was observed, largely driven by reporting from the banking and e-money sectors. The most common triggers for suspicion were adverse media and open-source intelligence (24%), followed by payment fraud indicators (16%) and Know Your Customer (KYC)-related concerns (15%). During operational analysis, a number of SARs were reclassified (most commonly to money laundering or fraud), reflecting ongoing refinement in analytical assessments.

SARs submitted in 2025 were connected to 85 jurisdictions, with 78% involving a United Kingdom nexus. Reports referencing Mexico declined sharply compared to previous years. Only 0.40% of SARs involved jurisdictions listed by the Financial Action Task Force as high-risk or subject to increased monitoring, indicating limited direct exposure to



listed jurisdictions within the reporting dataset.

A total of 172 SARs (2.9% of total submissions) were assessed as having a direct Gibraltar nexus. The banking sector accounted for 51% of these reports. Across Gibraltar-linked SARs, money laundering and fraud remained the predominant suspected offences.

The proportion of defensive SARs remained minimal at 0.25%, representing a substantial reduction from 25% recorded in 2019. This sustained improvement reflects the impact of the GFIU's targeted outreach programme, Project Nexus, and demonstrates enhanced reporting and improved intelligence quality across sectors.

Overall SAR quality remained consistently high. Where deficiencies were identified, structured feedback was provided to reporting entities to promote further improvement and reinforce compliance standards.

Section 4I disclosures under the Proceeds of Crime Act continued to increase in relevance. In 2025, 89 such disclosures were submitted across 12 sectors, compared to 24 submissions from three sectors in 2024. This mechanism is increasingly utilised to share intelligence that does not meet the formal SAR threshold but remains materially relevant to the disruption of financial crime.

The GFIU received 428 Defence Against Money Laundering (DAML) requests in 2025, representing a 5% increase from 2024. These requests were submitted across 11 sectors, with banking (176) and gaming (147) accounting for the highest volumes. The average response time was four working days.

Approximately 60% of DAML requests related to suspected money laundering, while approximately one quarter related to suspected fraud. DAML submissions were connected to activity across 45 jurisdictions, with the United Kingdom most frequently cited. In addition, three Defence Against Terrorist Financing (DATF) requests were submitted under the Terrorism Act 2018.

International cooperation remained strong. In 2025:

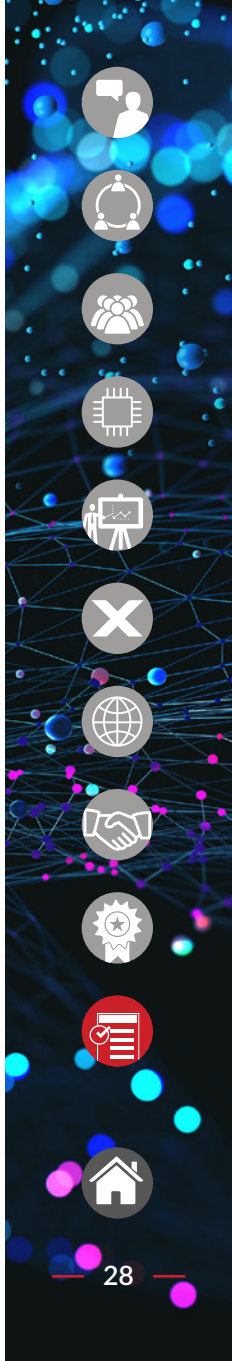
- 74 incoming Egmont requests were received from 34 jurisdictions (an 11% decrease from 2024),
- 66 outgoing Egmont requests were sent to 28 jurisdictions (a 38% increase),
- 8 non Egmont requests were received from seven jurisdictions,
- 15 incoming IACCC requests were received,
- 23 spontaneous intelligence reports were received from11 jurisdictions through Egmont, and
- 879 Egmont spontaneous intelligence reports were disseminated to 52 jurisdictions through Egmont.

Money laundering and fraud were the predominant suspected criminalities associated with international intelligence exchanges. Sexual exploitation cases, largely linked to VASP related reporting, ranked third among outgoing spontaneous intelligence disclosures. Despite the requirement for external consultation in the majority of cases, 62% of Egmont requests were responded to within the recommended 30 day timeframe.

Domestically, the introduction of a revised Joint Financial Intelligence Tasking Group (JFITG) process resulted in a marked increase in the frequency of inter-agency engagement. This operational enhancement contributed directly to a significant rise in intelligence dissemination.

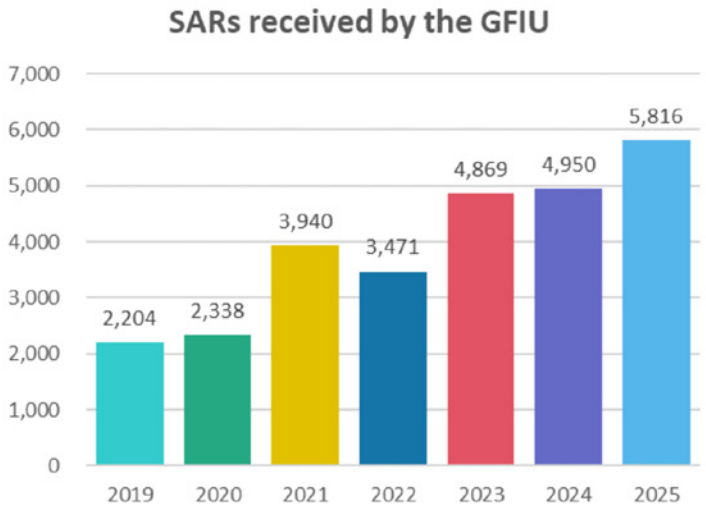
Disseminations increased by 154%, rising from 142 reports in 2024 to 361 in 2025. The majority related to suspected money laundering, fraud, tax offences, terrorist financing, and sanctions-related activity.

Overall, the 2025 reporting year demonstrates a sustained increase in SAR submissions, improved reporting quality, enhanced international cooperation, and increased operational outputs. The continued reduction in defensive reporting, the expanded use of Section 4I disclosures, and the rise in intelligence-led disseminations collectively reflect a more mature and risk-based regime.



Unless otherwise indicated, the statistical data presented in this report relates to the 2025 reporting year and is provided in comparison with 2024. All figures have been extracted from the GFIU's reporting platform, THEMIS, and analysed using dedicated analytical tools.

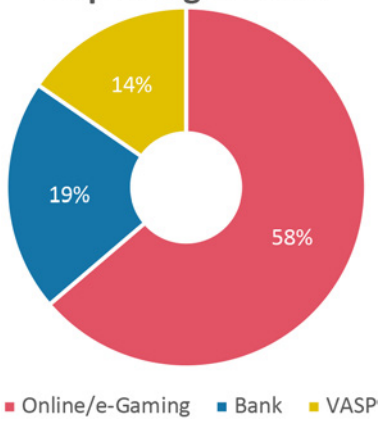
As THEMIS operates as a live database, the data reflects a snapshot in time extract. While any variance between this report and other GFIU publications is expected to be negligible, minor differences may arise as a result of subsequent system updates, data validation processes, or the inclusion of additional information following the reporting cut-off date.



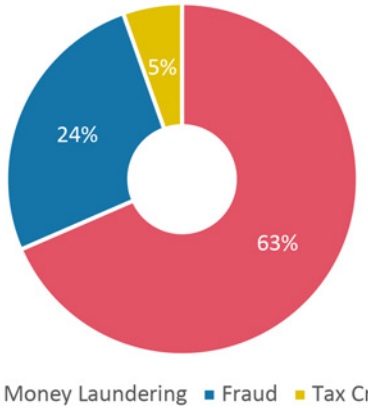
Crystal Reports are received from the UK Financial Intelligence Unit (UKFIU) and serve as an important data matching mechanism that strengthens the GFIU's analytical capability. These reports align and compare information across multiple datasets in order to identify potential matches, associations, or any nexus involving Gibraltar-based individuals, legal persons, or any other Gibraltar nexus.

Each report is subject to operational analysis using a methodology broadly consistent with that applied to SARs. The GFIU attaches significant value to these reports, recognising them as a high-impact source of financial intelligence that supports both strategic assessments and operational development. This intelligence-sharing arrangement reflects the strength and continuity of cooperation between the GFIU and the UKFIU.

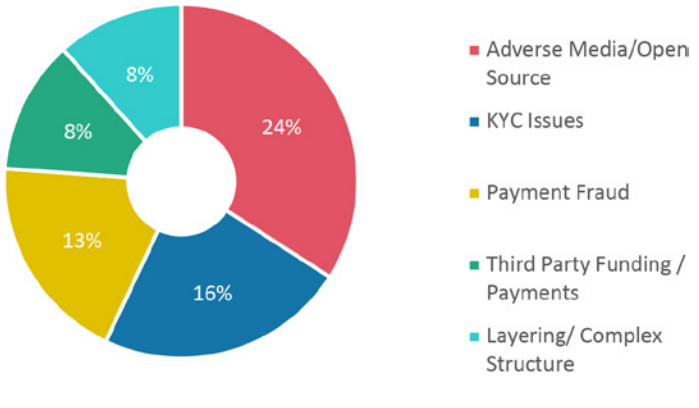
Reporting Sectors



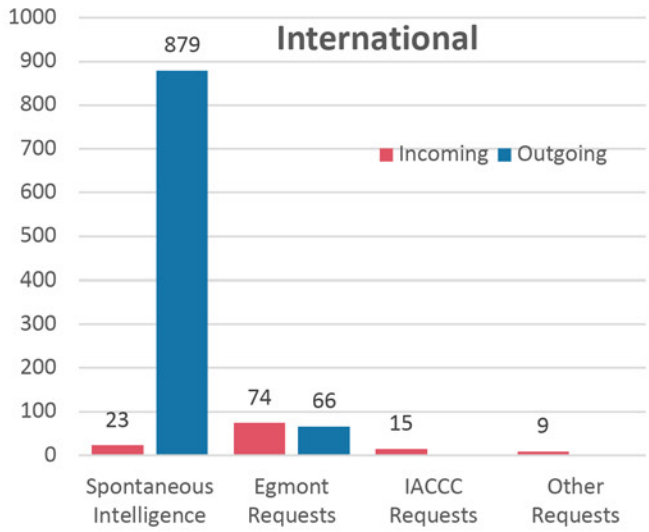
Suspected Criminality



Grounds for Suspicion

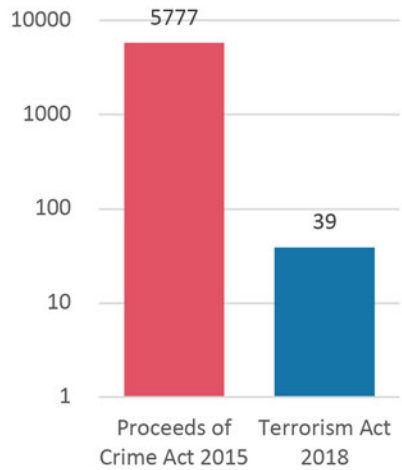


International



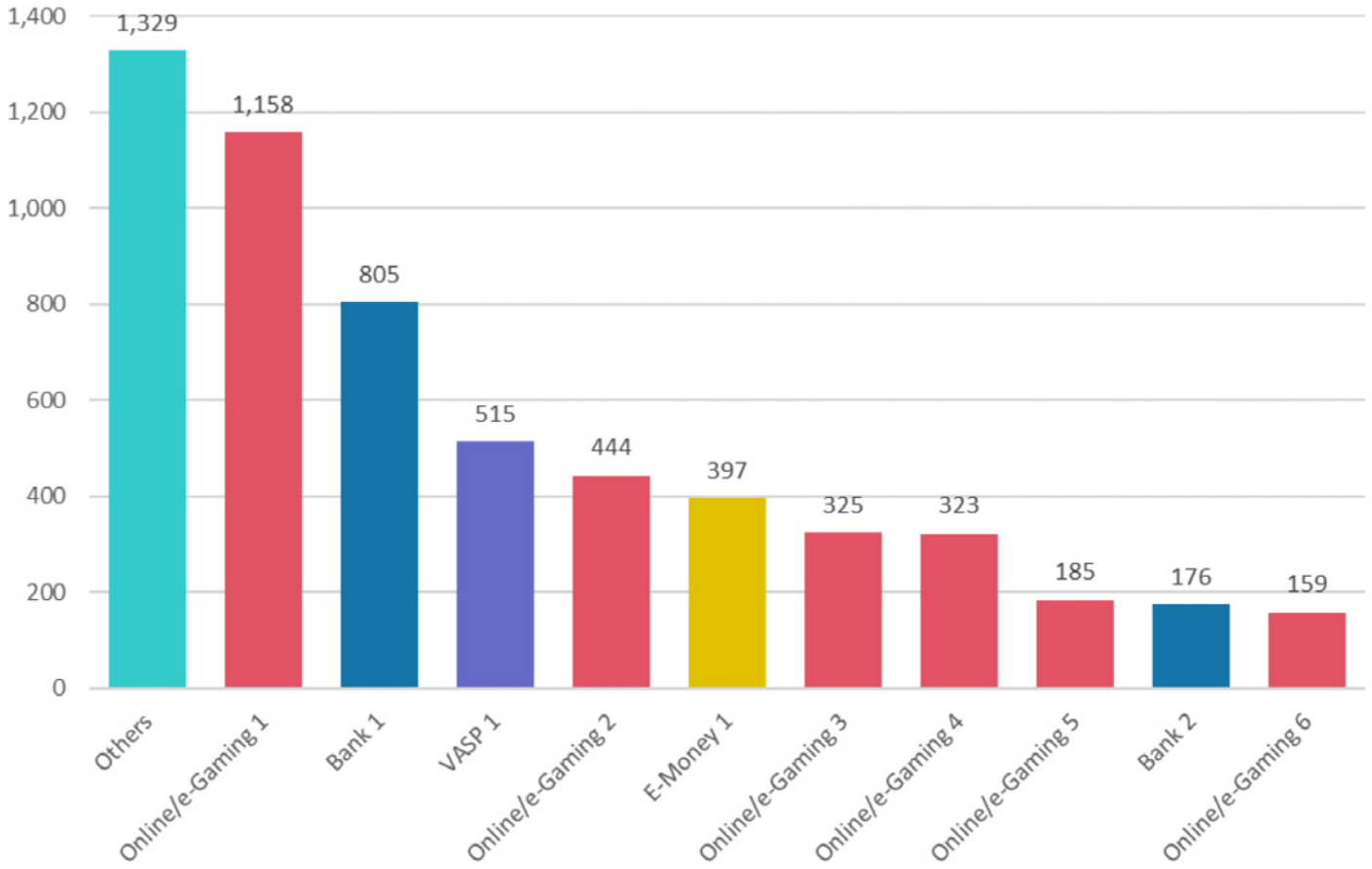
Local

SARs by Legislation



*Section 1DA/1DAA requests under the Proceeds of Crime are request to relevant financial business for relevant information.

In 2025 the top ten reporting entities accounted for 77% of the total SARs received.

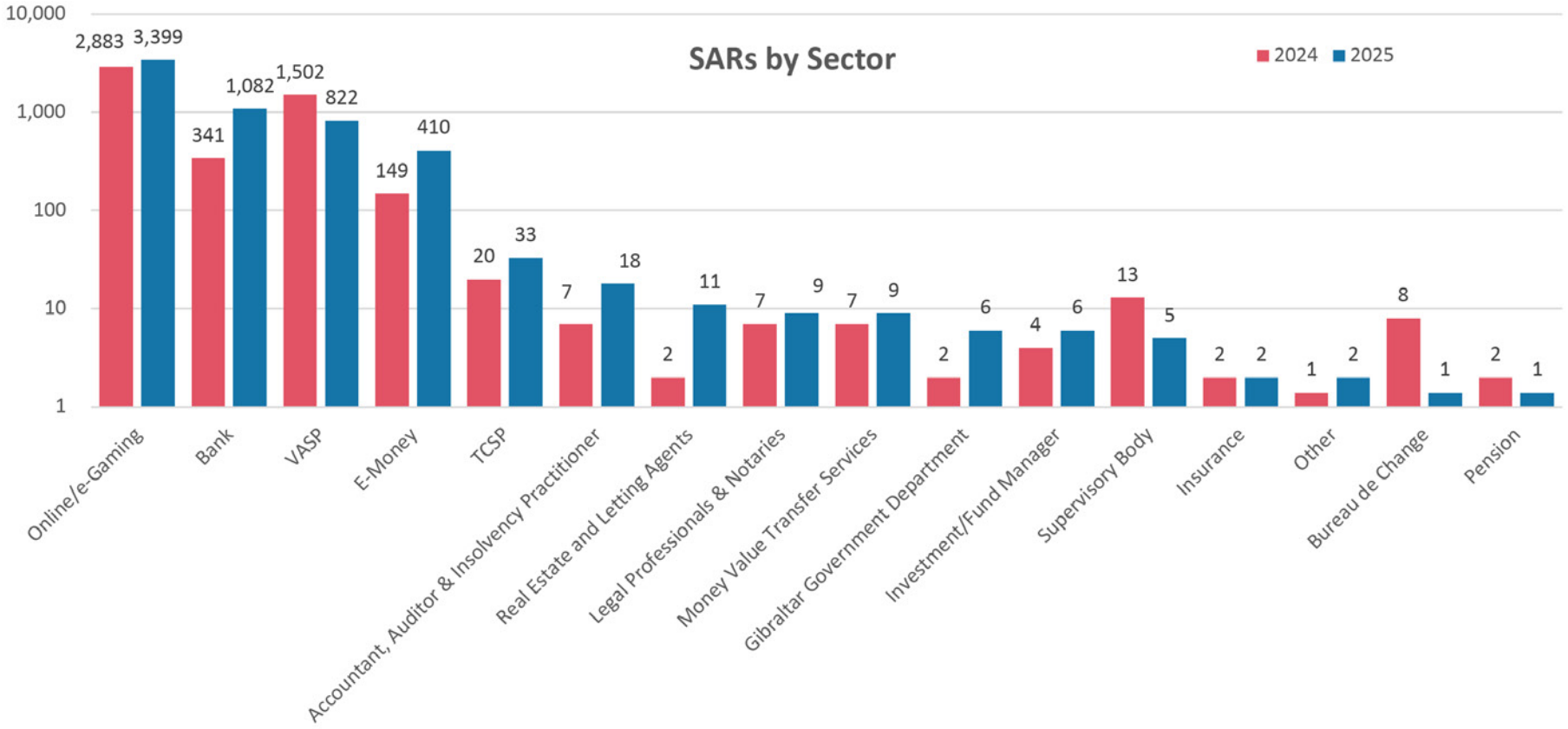


Reporting Sectors

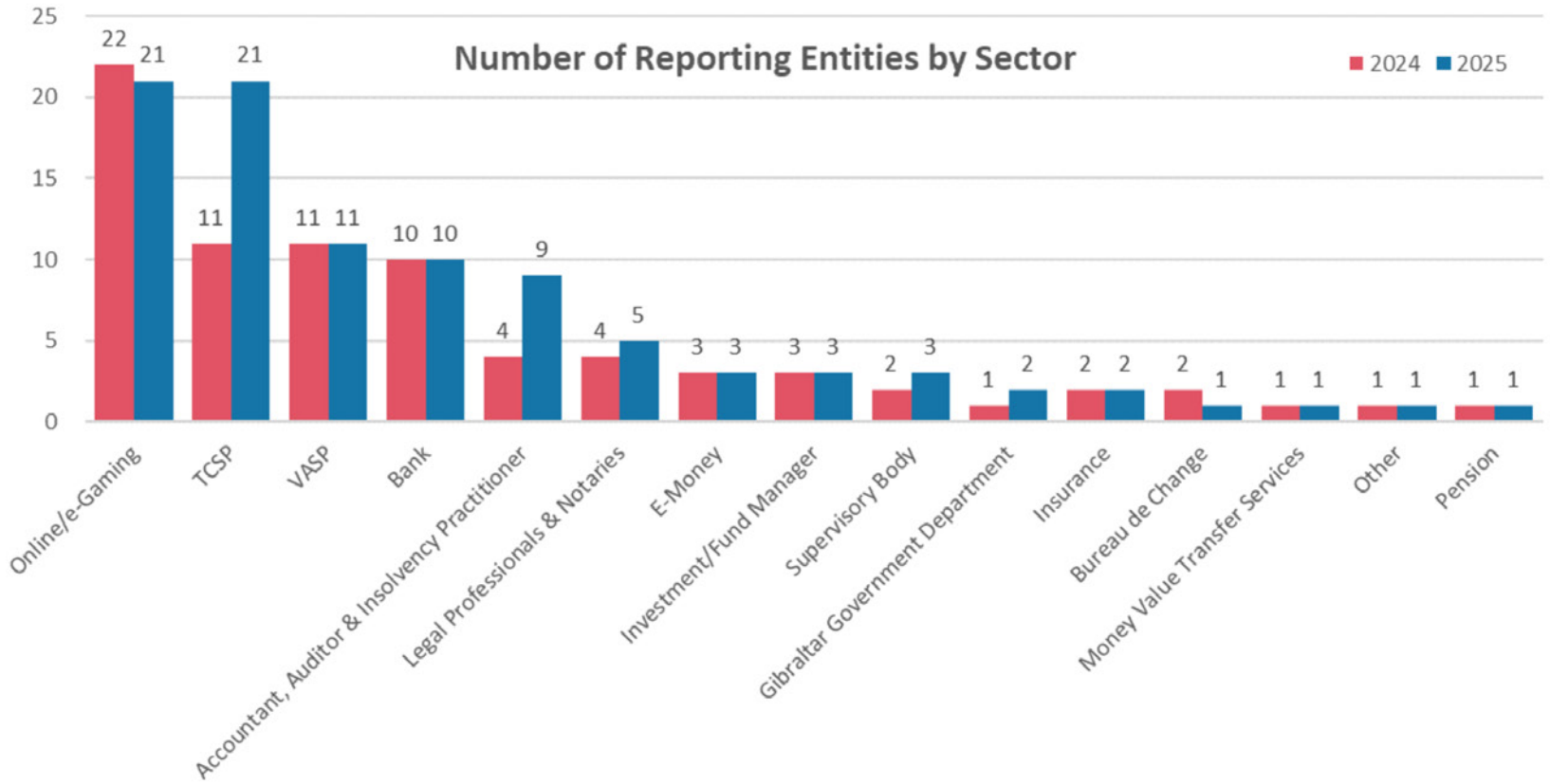
In 2025, a total of 5,816 SARs were submitted, representing a 17.49% increase compared with 2024.

Consistent with previous years, the gaming sector remained the largest contributor, filing 3,399 reports and accounting for 58% of all SARs received. This reflects an 18% rise in submissions from the sector compared to 2024. Notably, 90% of these reports were also dual-reported to foreign jurisdictions.

Meanwhile, the banking sector recorded a substantial 217% increase in SAR submissions compared to 2024, becoming the second-largest reporting sector and accounting for 19% of all SARs. By contrast, reporting from the VASP sector declined sharply by 45%, comprising 14% of total SARs.

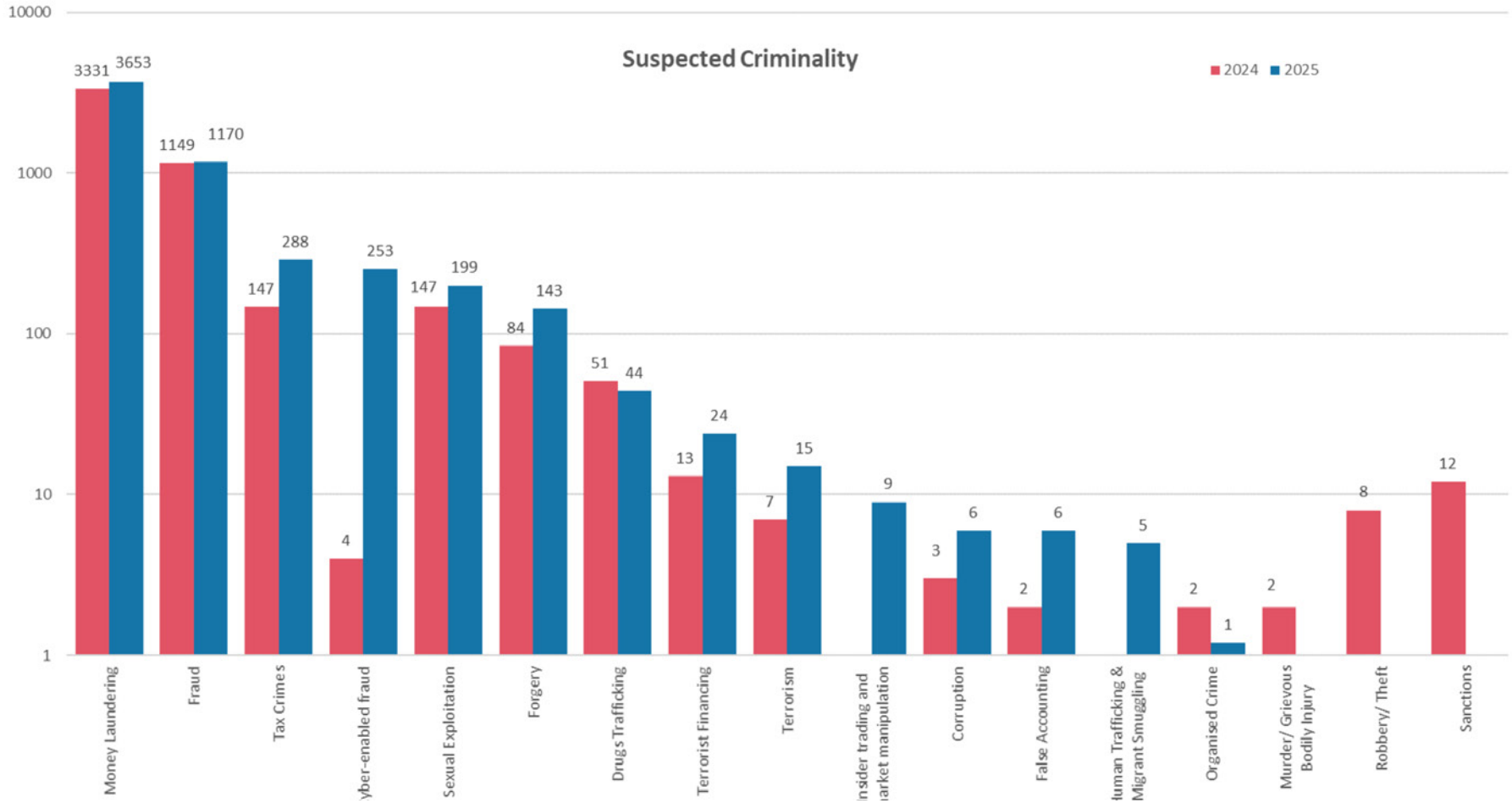


In 2025, a total of 99 reporting entities across 16 sectors submitted SARs, up from 80 entities in 2024. This growth is largely driven by an increase in reporting entities within the TCSP sector and the accountant, auditor & insolvency practitioner sectors.



Suspected Criminality

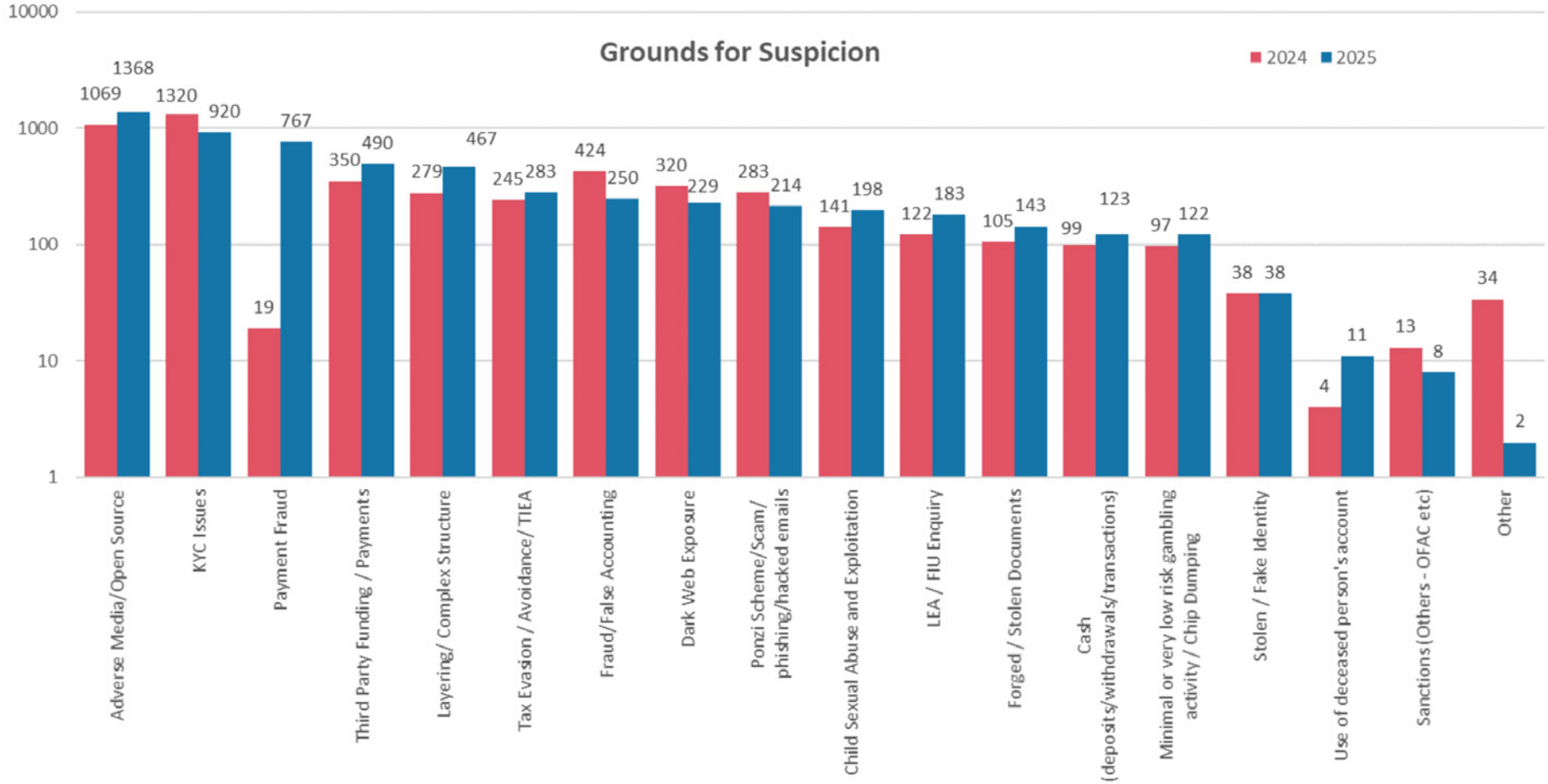
Consistent with previous reporting periods, the suspected criminality selected by reporters did not always align with the underlying activity that triggered the suspicion. During the assessment process, the categorisation of several SARs was amended most commonly to money laundering or fraud. Money laundering and fraud remain the predominant suspected criminal activities reported. A significant increase was observed in payment related and cyber-enabled fraud, largely driven by reporting from the banking and e-money sectors, highlighting the continued evolution of technology-facilitated financial crime typologies.



Sector/ Suspected Criminality	Corruption	Cyber-enabled fraud	Drugs Trafficking	False Accounting	Forgery	Fraud	Human Trafficking & Migrant Smuggling	Insider trading and market manipulation	Money Laundering	Organised Crime	Sexual Exploitation	Tax Crimes	Terrorism	Terrorist Financing	Total
Accountant, Auditor & Insolvency Practitioner	1	-	-	-	1	6	-	-	5	-	-	5	-	-	**18**
Bank	1	199	2	-	8	599	2	-	243	-	2	25	-	1	**1082**
Bureau de Change	-	-	-	-	-	-	-	-	1	-	-	-	-	-	**1**
E-Money	-	54	3	-	5	157	3	-	181	-	1	2	2	2	**410**
Gibraltar Government Department	-	-	-	-	1	1	-	-	-	-	-	4	-	-	**6**
Insurance	-	-	-	-	-	1	-	1	-	-	-	-	-	-	**2**
Investment/Fund Manager	1	-	-	-	-	1	-	-	4	-	-	-	-	-	**6**
Legal Professionals & Notaries	-	-	1	-	-	1	-	-	6	-	-	-	1	-	**9**
Money Value Transfer Services	-	-	-	-	-	-	-	-	9	-	-	-	-	-	**9**
Online/e-Gaming	-	-	1	-	120	213	-	8	2802	1	-	246	5	3	**3399**
Other	-	-	-	-	-	-	-	-	2	-	-	-	-	-	**2**
Pension	-	-	-	-	-	-	-	-	-	-	-	1	-	-	**1**
Real Estate and Letting Agents	-	-	-	1	2	2	-	-	6	-	-	-	-	-	**11**
Supervisory Body	-	-	-	-	-	2	-	-	1	-	-	2	-	-	**5**
TCSP	1	-	-	5	2	8	-	-	15	-	-	1	1	-	**33**
VASP	2	-	37	-	4	179	-	-	378	-	196	2	6	18	**822**
Total	**6**	**253**	**44**	**6**	**143**	**1170**	**5**	**9**	**3653**	**1**	**199**	**288**	**15**	**24**	**5816**

Grounds for Suspicion

In 2025, 24% of SARs were filed based on adverse media and open source intelligence findings, making this the most common reporting trigger. KYC-related concerns accounted for 15% of reports, largely due to inadequate customer identification details and insufficient source of funds documentation. Suspected payment fraud represented 16% of SARs, with most reports originating from the banking and e-money sectors.



Sector / Grounds for Suspicion	Adverse Media/Open Source	Cash (deposits/withdrawals/transactions)	Child Sexual Abuse and Exploitation	Dark Web Exposure	Forged / Stolen Documents	Fraud/False Accounting	Gambling	KYC Issues	Layering/ Complex Structure	LEA / FIU Enquiry	Payment Fraud	Ponzi Scheme/Scam/phishing/hacked emails	Stolen / Fake Identity	Tax Evasion / Avoidance/ TIEA	Third Party Funding / Payments	Use of deceased person's account	Other	Total
Accountant, Auditor & Insolvency Practitioner	3	-	-	-	1	5	-	1	2	-	-	-	-	5	-	-	1	**18**
Bank	10	15	2	4	8	64	-	24	67	16	603	114	4	20	126	2	3	**1,082**
Bureau de Change	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	**1**
E-Money	20	12	-	-	5	48	-	28	77	19	145	6	-	2	47	-	1	**410**
Gibraltar Government Department	-	-	-	-	1	1	-	-	-	-	-	-	-	4	-	-	-	**6**
Insurance	1	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	**2**
Investment/Fund Manager	2	-	-	1	-	-	-	-	2	-	-	-	-	-	-	-	-	**6**
Legal Professionals & Notaries	3	-	-	-	-	1	-	2	2	-	-	-	-	-	1	-	1	**9**
Money Value Transfer Services	-	3	-	-	-	-	-	3	2	-	-	-	-	-	1	-	-	**9**
Online/e-Gaming	1302	91	-	-	121	106	122	816	112	135	7	-	32	246	300	9	-	**3,399**
Other	-	1	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	**2**
Pension	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	**1**
Real Estate and Letting Agents	5	-	-	-	2	1	-	3	-	-	-	-	-	-	-	-	-	**11**
Supervisory Body	1	-	-	-	-	1	-	-	-	1	-	-	-	2	-	-	-	**5**
TCSP	11	1	-	-	2	7	-	7	1	1	-	-	-	1	1	-	1	**33**
VASP	10	-	196	225	4	16	-	32	201	11	12	94	2	2	14	-	3	**822**
Total	**1,368**	**123**	**198**	**230**	**144**	**250**	**122**	**918**	**467**	**183**	**767**	**214**	**38**	**283**	**490**	**11**	**10**	**5,816**

SARs with a Gibraltar nexus

In 2025, a total of 172 SARs were assessed as having a Gibraltar nexus, accounting for 2.9% of all reports received. The banking sector was the primary contributor, submitting 88 of these SARs, which represents 51% of the Gibraltar linked reports.

Overall, SARs with a Gibraltar nexus were submitted by 14 different sectors.

Sector/ Suspected Criminality	Corruption	Cyber-enabled fraud	Drugs Trafficking	False Accounting	Forgery	Fraud	Insider trading and market manipulation	Money Laundering	Tax Crimes	Total
Accountant, Auditor & Insolvency Practitioner	-	-	-	-	1	2	-	5	5	**13**
Bank	1	3	1	-	1	14	-	49	19	**88**
Bureau de Change	-	-	-	-	-	-	-	1	-	**1**
E-Money	-	-	-	-	-	-	-	2	-	**2**
Gibraltar Government Department	-	-	-	-	1	1	-	-	3	**5**
Insurance	-	-	-	-	-	-	1	-	-	**1**
Investment/Fund Manager	1	-	-	-	-	1	-	2	-	**4**
Legal Professionals & Notaries	-	-	1	-	-	-	-	5	-	**6**
Money Value Transfer Services	-	-	-	-	-	-	-	9	-	**9**
Online/e-Gaming	-	-	-	-	-	-	-	1	-	**1**
Real Estate and Letting Agents	-	-	-	1	2	2	-	6	-	**11**
Supervisory Body	-	-	-	-	-	1	-	-	1	**2**
TCSP	1	-	-	4	1	6	-	14	1	**27**
VASP	1	-	-	-	-	-	-	1	-	**2**
Total	**4**	**3**	**2**	**5**	**6**	**27**	**1**	**95**	**29**	**172**

Defensive SARs

Defensive SARs describe a recognised reporting practice whereby entities apply overly broad or precautionary detection criteria in order to mitigate perceived regulatory, compliance, or reputational exposure. Such reports are typically identified during the GFIU's operational analysis stage where the underlying activity or transaction is assessed as not meeting the threshold of suspicion, or where the suspicion articulated by the reporting entity is not substantiated by the available facts.

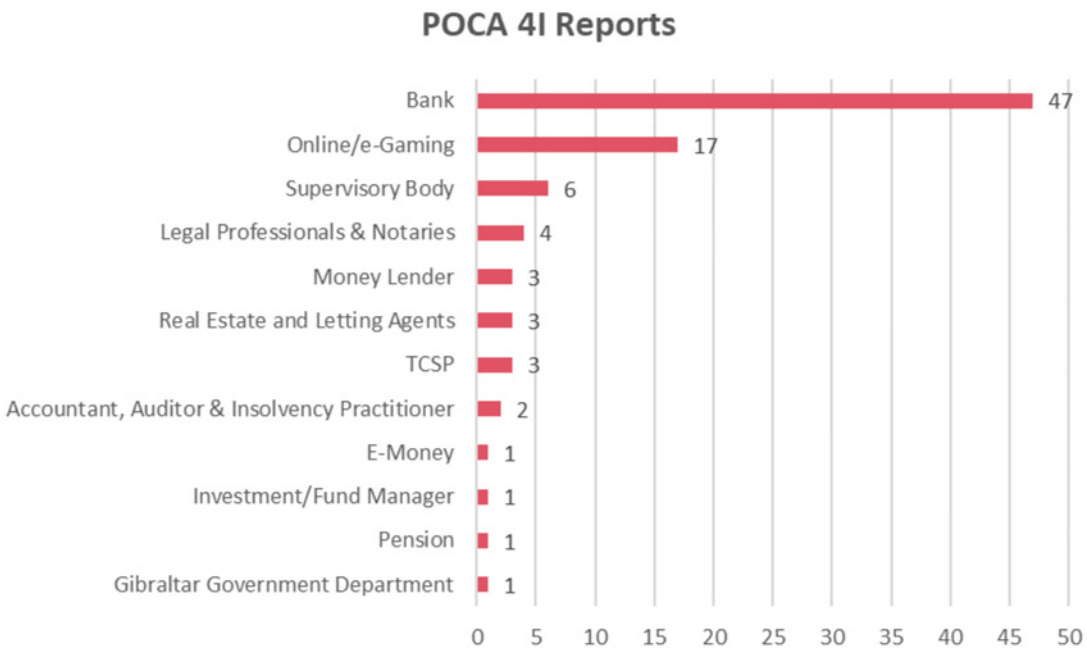
The submission of defensive SARs can adversely affect the overall effectiveness of the reporting regime by mischaracterising legitimate conduct as suspicious, thereby diluting analytical focus and reducing the intelligence value of disclosures.

Through sustained engagement under its targeted outreach initiative, Project Nexus, the GFIU has achieved a marked reduction in defensive reporting. In 2025, only 0.25% of SARs processed were classified as defensive, compared to 25% in 2019. This significant decline reflects improved reporting precision and supports a more proportionate, risk-based, and intelligence-led SAR framework, thereby reinforcing the integrity and operational utility of the regime.

POCA Section 4I Reports

Under the Proceeds of Crime Act 2015 (Section 4I) reporting entities can voluntarily disclose information if it is made for the purposes of the exercise of a GFIU function. This provision ensures that even if it does not meet the threshold for a SAR, the information can contribute to tackle financial crime or other criminal conduct. While still considered a recent addition to the legislative framework, Section 4I, has become an extremely valuable tool for enhancing our knowledge and intelligence capabilities.

In 2025, a total of 89 reports were filed under Section 4I of POCA, submitted by 12 reporting sectors. This marks a substantial rise compared to 2024, when 24 reports were received from three sectors.

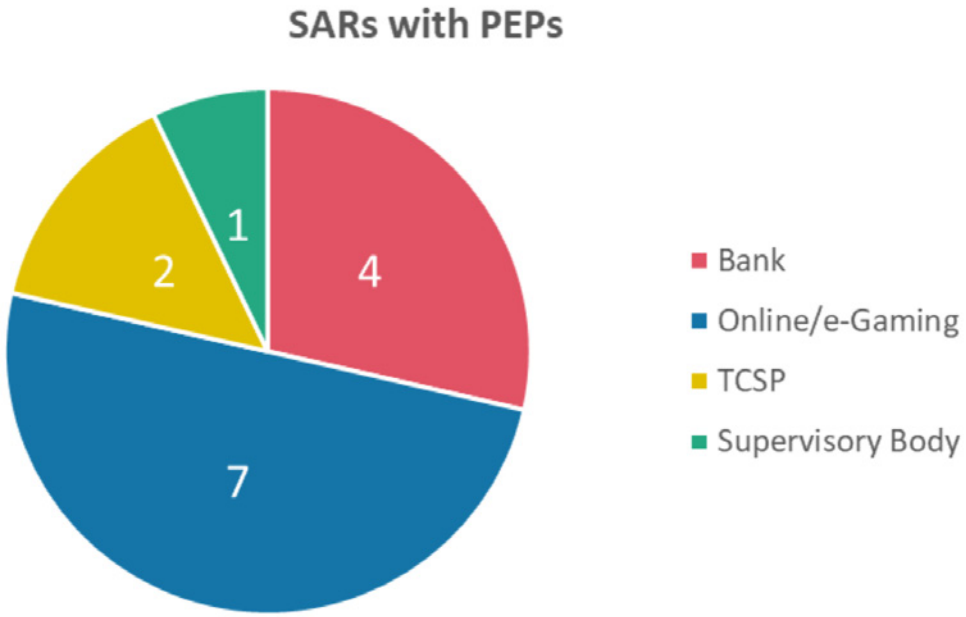


Politically Exposed Persons

When submitting a SAR, MLROs are required to report any links to, or identification of, Politically Exposed Persons (PEPs). A review of historical SARs involving PEP subjects revealed that some individuals had been misclassified. Upon further analysis, these individuals were more accurately identified as Media Exposed Persons (MEPs), and their classifications were updated accordingly.

In 2025, 14 SARs were filed identifying a PEP as a subject, the same number reported in 2024.

The chart shows the numbers of PEP connected SARs per sector submitted during 2025.



Consent Requests

Although "consent" is the formal terminology prescribed under the relevant legislative framework, the GFIU adopts the term "Defence Against Money Laundering" (DAML) requests to provide greater clarity and practical understanding for stakeholders.

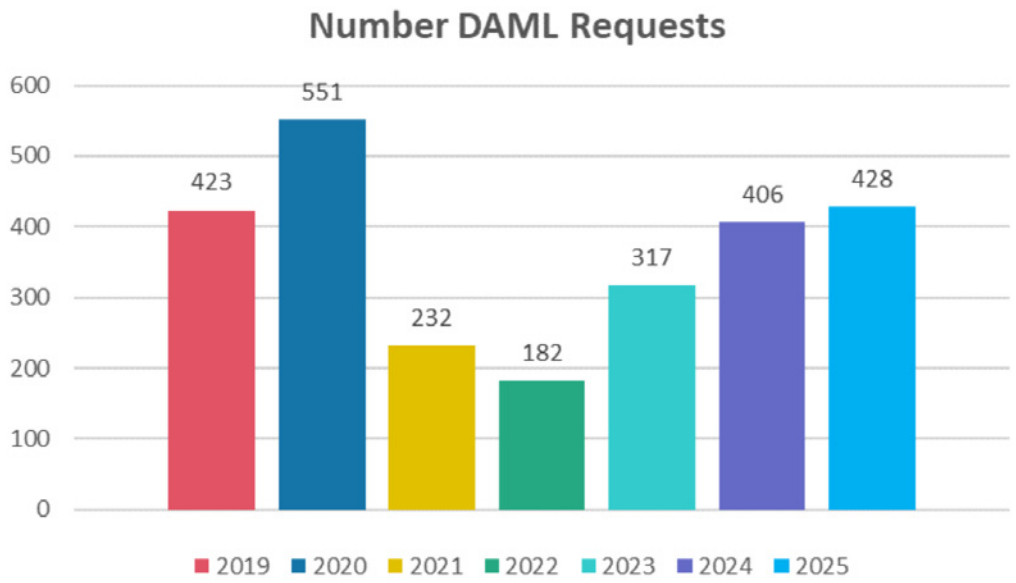
DAML requests are submitted by reporting entities when they seek a statutory defence prior to proceeding with a transaction suspected to involve criminal property. This mechanism enables the GFIU to assess the underlying suspicion, determine whether the statutory threshold is met, and consider whether further operational action, including restraint or investigative referral, is required before the transaction proceeds.

In 2025, the GFIU received 428 DAML requests, including those linked to SARs filed in previous years. This represents a 5% increase from 2024, continuing the upward trend observed that year.

DAML requests were submitted across 11 reporting sectors in 2025, with the highest volumes coming from the banking sector (176 requests) and the gaming sector (147 requests). The GFIU maintained an average response time of four working days, ensuring timely handling of these sensitive matters.

Of the 1,082 SARs submitted by the banking sector in 2025, 126 included DAML requests, constituting approximately 12% of all filings. Several of these SARs contained multiple DAML requests. This highlights the sector's sustained and proactive role in identifying suspected criminal property.

In 2025, three Defence Against Terrorist Financing (DATF) requests were submitted under the Terrorism Act 2018. One request from the TCSP sector was initially refused but later granted a defence. Two requests originated from the VASP sector; one was granted a defence, while the other was deemed not applicable.



A total of 38 DAML requests received a 'not applicable' response. These were cases where either the request did not pertain to a prohibited act under the Proceeds of Crime Act (POCA), or where insufficient information was provided, despite follow up requests from the GFIU for the necessary details.

Seven DAML requests received no reply, either because they were submitted in error, later withdrawn, or treated as having implied consent.

Sector	DAML Granted	DAML Not Applicable	DAML Refused	DAML Rescinded	DAML Subsequently Granted	No Response Required	Total
Accountant, Auditor & Insolvency Practitioner	2	6	-	-	-	-	**8**
Bank	162	8	6	-	-	-	**176**
E-Money	17	2	-	-	-	-	**19**
Insurance	1	2	-	-	-	-	**3**
Investment/Fund Manager	1	-	-	-	-	-	**1**
Legal Professionals & Notaries	-	1	-	-	-	-	**1**
Online/e-Gaming	132	9	1	1	1	3	**147**
Pension	1	-	-	-	-	-	**1**
Real Estate and Letting Agents	2	2	1	-	-	-	**5**
TCSP	9	6	-	-	-	1	**16**
VASP	46	2	-	-	-	3	**51**
Total	**373**	**38**	**8**	**1**	**1**	**7**	**428**

Slightly more than 60% of the DAML requests received were connected to SARs related to suspected money laundering, while about one quarter were linked to suspected fraud.

Suspected Criminality	DAML Granted	DAML Not Applicable	DAML Refused	DAML Rescinded	DAML Subsequently Granted	No Response Required	Total
Corruption	4	1	-	-	-	-	**5**
Cyber-enabled fraud	4	-	-	-	-	-	**4**
False Accounting	-	1	-	-	-	-	**1**
Forgery	12	1	-	-	-	-	**13**
Fraud	83	11	6	-	-	-	**100**
Human Trafficking & Migrant Smuggling	-	3	-	-	-	-	**3**
Insider trading and market manipulation	4	2	-	-	-	-	**6**
Money Laundering	235	17	2	1	1	6	**262**
Sexual Exploitation	1	-	-	-	-	1	**2**
Tax Crimes	30	2	-	-	-	-	**32**
Total	**373**	**38**	**8**	**1**	**1**	**7**	**428**

In 2025, there were 357 SARs that had DAML requests, 44 of which involved more than one request. The banking sector submitted the highest number of SARs with multiple consent requests, including three SARs that each resulted in five separate requests.

The table below outlines the number of consent requests received in 2025 by sector, along with the number of consent requests per SAR.

	Number of DAML requests per SAR					
Row Labels	**1**	**2**	**3**	**4**	**5**	**Total**
Accountant, Auditor & Insolvency Practitioner	2	3	-	-	-	**5**
Bank	118	11	7	-	3	**139**
E-Money	17	1	-	-	-	**18**
Insurance	-	-	1	-	-	**1**
Investment/Fund Manager	1	-	-	-	-	**1**
Legal Professionals & Notaries	1	-	-	-	-	**1**
Online/e-Gaming	130	5	1	1	-	**137**
Pension	1	-	-	-	-	**1**
Real Estate and Letting Agents	5	-	-	-	-	**5**
TCSP	6	2	2	-	-	**10**
VASP	29	9	-	1	-	**39**
Total	**310**	**31**	**11**	**2**	**3**	**357**

DAML requests received in 2025 were associated with activities spanning 45 jurisdictions where the suspicion arose. Of those with a Gibraltar nexus, three fifths were submitted by the banking sector.

The table below shows the top seven jurisdictions.

Jurisdiction	Accountant, Auditor & Insolvency Practitioner	Bank	E-Money	Insurance	Legal Professionals & Notaries	Online/e-Gaming	Real Estate and Letting Agents	TCSP	VASP	Total
United Kingdom	2	40	17			81		2	11	153
Gibraltar	2	30		3	1		5	11	1	53
Colombia		33							2	35
Canada		1				32				33
Italy		12							1	13
Brazil		2				7			3	12
Ireland						10			2	12

Each of the remaining jurisdictions recorded fewer than 10 DAML requests.

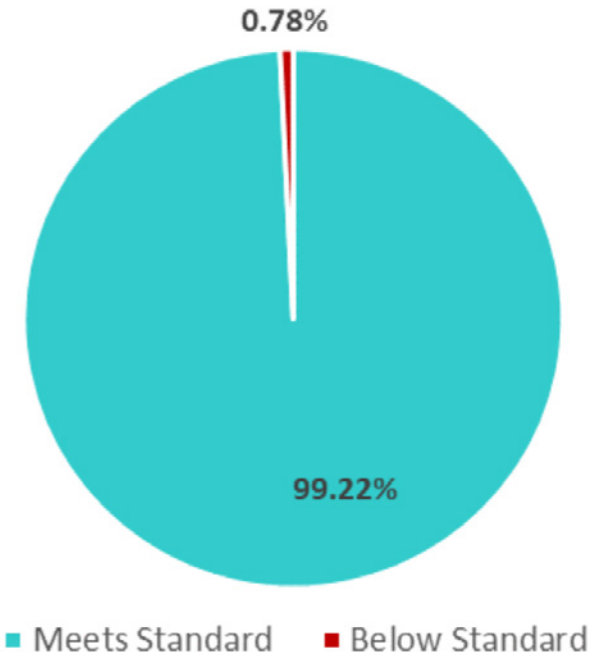
Findings of the Feedback Provided to the Reporter

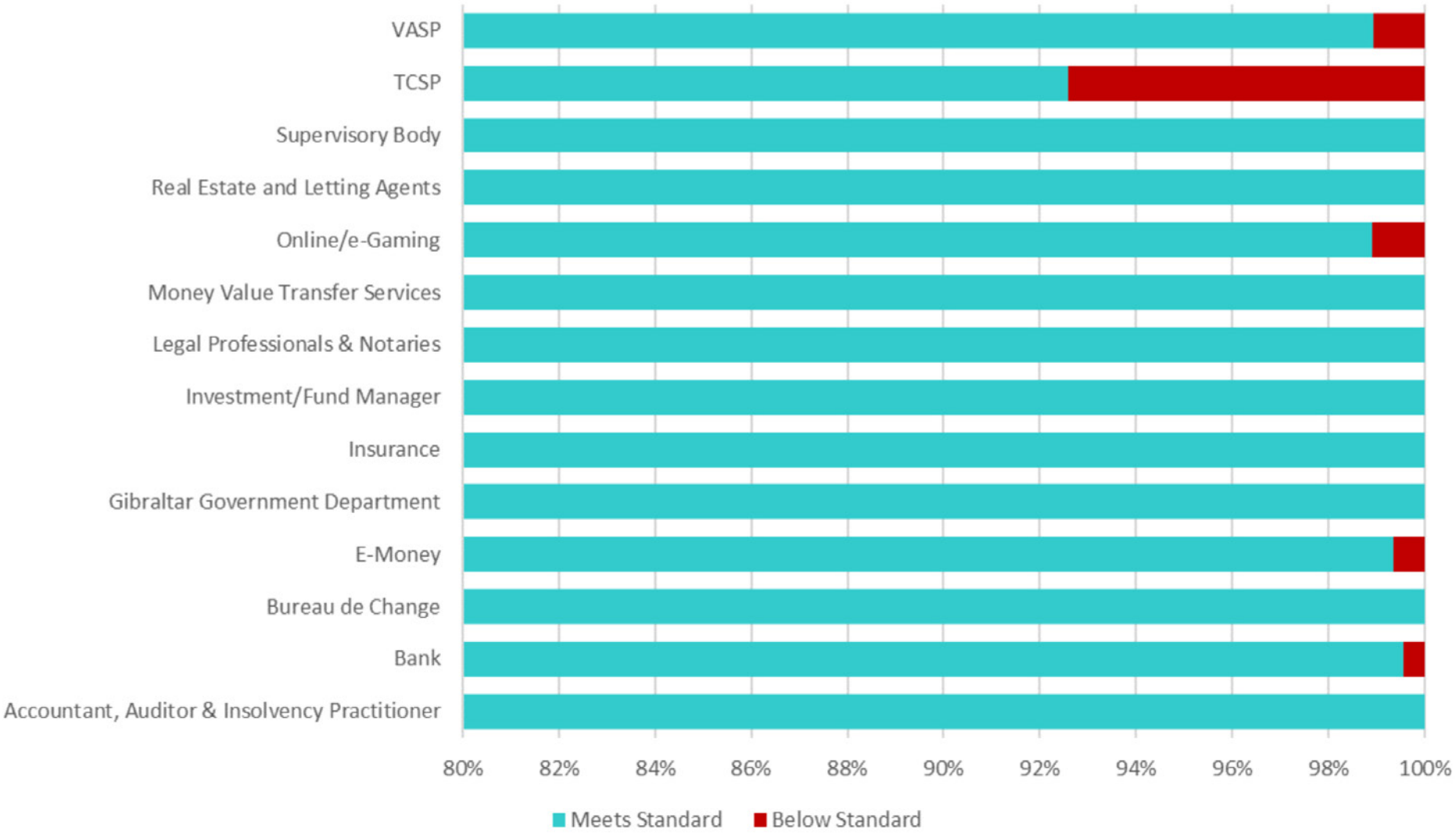
Quality feedback provided to the Reporter [Money Laundering Reporting Officer/ Nominated Officer] comprises ratings given for the following five criteria.

- Supporting documentation necessary for the GFIU must be submitted with the SAR for the effective analysis of the information disclosed.
- There must be a suspicion of a predicate offence, money laundering or terrorist financing within the information disclosed to GFIU.
- All background information contained in the SAR on the relationship with the reported subject must be described in sufficient detail.
- The content of the information must be clear and complete.
- When Consent has been requested, the information contained within the request must include the suspicion (within the narrative of the grounds for suspicion), the criminal property and the prohibited act.

The proportion of SARs assessed as meeting the required standard remains consistently high, highlighting the effectiveness of the GFIU's outreach efforts in enhancing SAR quality.

For SARs graded below standard, feedback was provided outlining the reasons for the assessment and suggestions for improvement.




VASP
TCSP
Supervisory Body
Real Estate and Letting Agents
Online/e-Gaming
Money Value Transfer Services
Legal Professionals & Notaries
Investment/Fund Manager
Insurance
Gibraltar Government Department
E-Money
Bureau de Change
Bank
Accountant, Auditor & Insolvency Practitioner
80%
82%
84%
86%
88%
90%
92%
94%
96%
98%
100%
Meets Standard
Below Standard

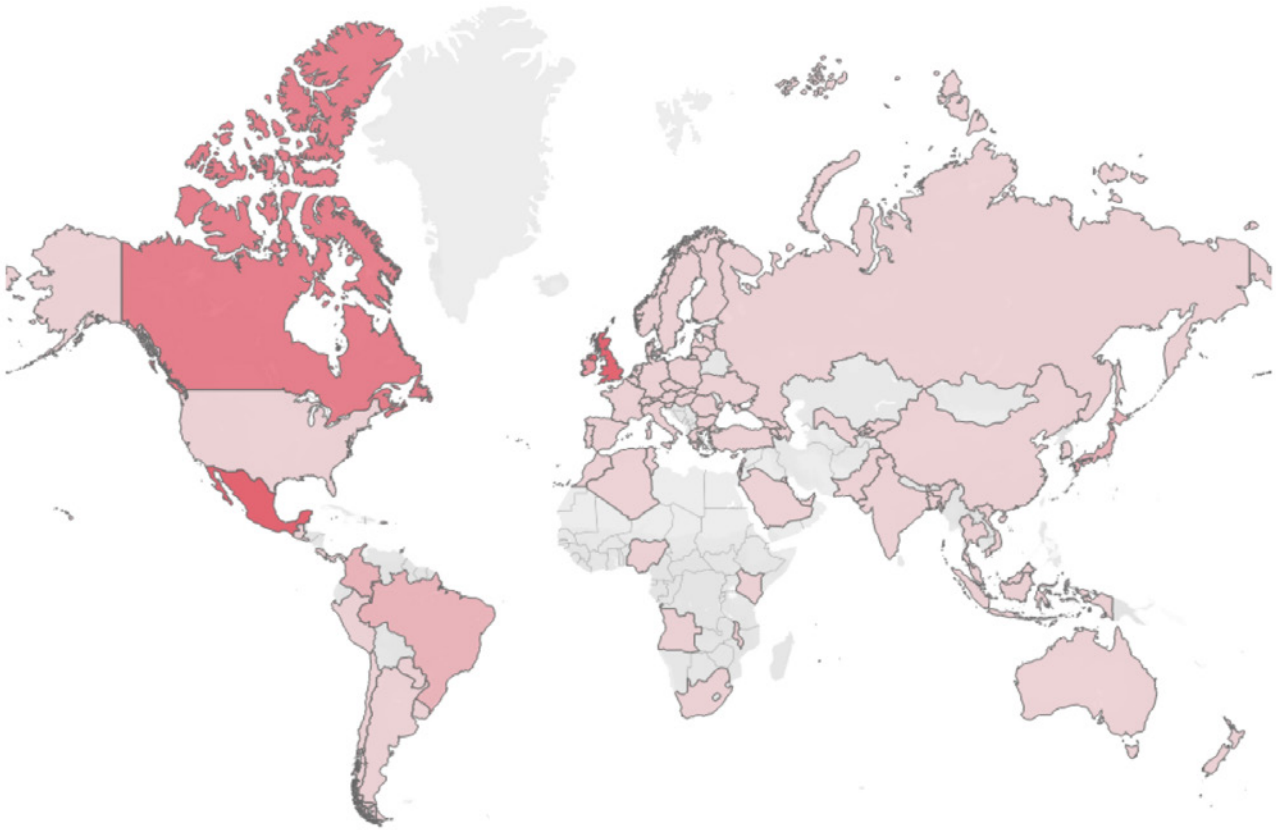
SARs Reported by Jurisdiction

In 2025, SARs demonstrated connectivity to 85 jurisdictions, reflecting the continued cross border dimension of financial activity processed through Gibraltar-based entities. Consistent with previous reporting periods, the United Kingdom remained the predominant geographic nexus, referenced in 78% of reports. These were largely submitted by the gaming, banking, and e-money sectors.

The most frequently cited suspected criminalities associated with international linkages were money laundering, fraud, and tax-related offences.

Reports involving a Mexican nexus declined significantly compared to prior years. The limited number recorded in 2025 originated almost exclusively from the VASP sector and were primarily associated with suspected money laundering and cases involving child sexual abuse and exploitation.

The chart shows a heat map of the SARs received in 2025 per jurisdiction where the grounds of suspicion apply.



The following table shows the suspected criminality of SARs disclosed against the top ten jurisdictions where the crime was suspected to have occurred.

Jurisdiction	Corruption	Cyber-enabled fraud	Drugs Trafficking	False Accounting	Forgery	Fraud	Human Trafficking & Migrant Smuggling	Insider trading and market manipulation	Money Laundering	Organised Crime	Sexual Exploitation	Tax Crimes	Terrorism	Terrorist Financing	Total
United Kingdom	-	239	37	-	115	955	4	8	2732	1	11	219	7	4	**4,332**
Mexico	-	-	3	-	-	30	-	-	228	-	126	-	5	16	**408**
Canada	-	-	-	-	2	10	-	-	203	-	-	20	1	-	**236**
Gibraltar	4	3	2	5	6	27	-	1	95	-	-	29	-	-	**172**
Ireland	-	-	-	-	6	5	-	-	107	-	-	3	-	-	**121**
Colombia	-	-	-	-	2	4	-	-	74	-	2	-	-	-	**82**
Japan	-	-	-	-	-	65	-	-	16	-	-	-	-	-	**81**
Brazil	-	-	-	-	1	6	-	-	27	-	39	-	-	1	**74**
Argentina	-	2	-	-	-	3	-	-	18	-	13	-	1	-	**37**
New Zealand	-	-	-	-	2	1	-	-	19	-	-	-	-	-	**22**
Total	**4**	**244**	**42**	**5**	**134**	**1,106**	**4**	**9**	**3,519**	**1**	**191**	**271**	**14**	**21**	**5,565**

85 Jurisdictions in total.

The following table shows the suspected criminality of SARs disclosed against the top ten countries where the crime was suspected to have occurred, when SARs from the gaming sector are excluded.

Jurisdiction	Corruption	Cyber-enabled fraud	Drugs Trafficking	False Accounting	Forgery	Fraud	Human Trafficking & Migrant Smuggling	Insider trading and market manipulation	Money Laundering	Sexual Exploitation	Tax Crimes	Terrorism	Terrorist Financing	Total
United Kingdom	-	239	36	-	10	761	4	-	307	11	6	3	2	**1,379**
Mexico	-	-	3	-	-	30	-	-	228	126	-	5	16	**408**
Gibraltar	4	3	2	5	6	27	-	1	94	-	29	-	-	**171**
Colombia	-	-	-	-	2	4	-	-	74	2	-	-	-	**82**
Japan	-	-	-	-	-	65	-	-	16	-	-	-	-	**81**
Brazil	-	-	-	-	1	6	-	-	17	39	-	-	1	**64**
Argentina	-	2	-	-	-	3	-	-	18	13	-	1	-	**37**
Italy	-	1	-	-	-	4	-	-	13	-	-	-	-	**18**
Spain	-	2	-	-	-	4	-	-	6	-	3	-	-	**15**
France	-	-	-	1	-	2	-	-	10	-	-	-	-	**13**
Total	**4**	**247**	**41**	**6**	**19**	**906**	**4**	**1**	**783**	**191**	**38**	**9**	**19**	**2,268**

69 Jurisdictions in total.

The following table shows the reporting sector of SARs disclosed against the top ten jurisdictions where the crime was deemed to have occurred.

Jurisdiction	Accountant, Auditor & Insolvency Practitioner	Bank	Bureau de Change	E-Money	Gibraltar Government Department	Insurance	Investment/Fund Manager	Legal Professionals & Notaries	Money Value Transfer Services	Online/e-Gaming	Other	Pension	Real Estate and Letting Agents	Supervisory Body	TCSP	VASP	Total
United Kingdom	3	824	-	405	-	-	-	1	-	2953	-	-	-	2	1	143	**4,332**
Mexico	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	407	**408**
Canada	-	1	-	-	-	-	1	-	-	233	-	-	-	-	-	1	**236**
Gibraltar	13	88	1	2	5	1	4	6	9	1	-	-	11	2	27	2	**172**
Ireland	-	1	-	-	-	-	-	-	-	116	-	-	-	-	-	4	**121**
Colombia	-	57	-	-	-	-	-	-	-	-	-	-	-	-	-	25	**82**
Japan	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	81	**81**
Brazil	-	4	-	-	-	-	-	-	-	10	-	-	-	-	-	60	**74**
Argentina	-	5	-	-	-	-	-	-	-	-	-	-	-	-	-	32	**37**
New Zealand	-	-	-	-	-	-	-	-	-	22	-	-	-	-	-	-	**22**
Total	**16**	**981**	**1**	**407**	**5**	**1**	**5**	**7**	**9**	**3,335**	**0**	**0**	**11**	**4**	**28**	**755**	**5,565**

High Risk and Increased Monitoring rated Jurisdictions

The Financial Action Task Force ("FATF") identify jurisdictions with weak measures to combat money laundering and terrorist financing and issue these in public documents. The aim behind this process is to publicly list countries with weak AML/CFT regimes, with the aim to encourage the listed countries to make necessary reforms to their AML/CFT systems and redress weaknesses. These lists also provide useful information to stakeholders when risk assessing clients and transactions.

Note that the jurisdictions in the table below are as per the FATF lists published on 19 June 2026. Other jurisdictions are on the lists but are not mentioned in reports received by the GFIU, therefore they have been excluded from the report.

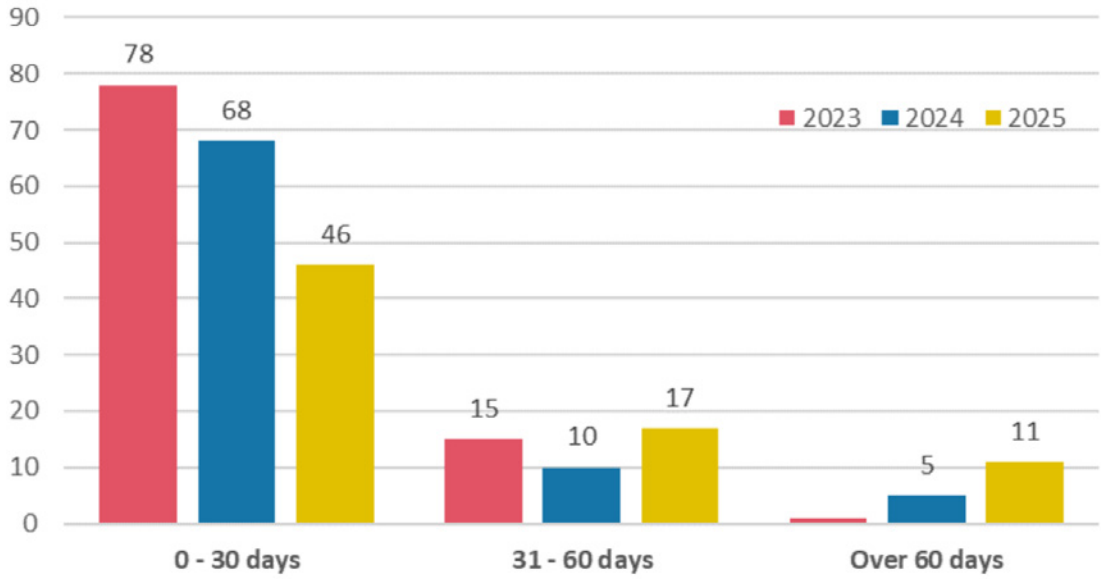
FATF high risk and increased monitoring rated jurisdictions	No. of SARs
Angola	4
Bulgaria	2
Kenya	1
Kuwait	2
Lebanon	1
Monaco	1
Viet Nam	1
No. of SARS with a link to a FATF high risk and increased monitoring rated jurisdictions	**12**
Total number of SARs	**5816**
% of SARs reported with link to a FATF high risk and increased monitoring rated jurisdictions	**0.21%**

Egmont Requests and Spontaneous Intelligence

Egmont requests comprise formal intelligence enquiries submitted by foreign FIUs seeking information held by the GFIU, accessible databases, or relevant third parties. These exchanges are conducted through the Egmont Secure Web and are recorded within THEMIS, enabling subject matching against existing GFIU data as well as cross-referencing with MLA requests where relevant.

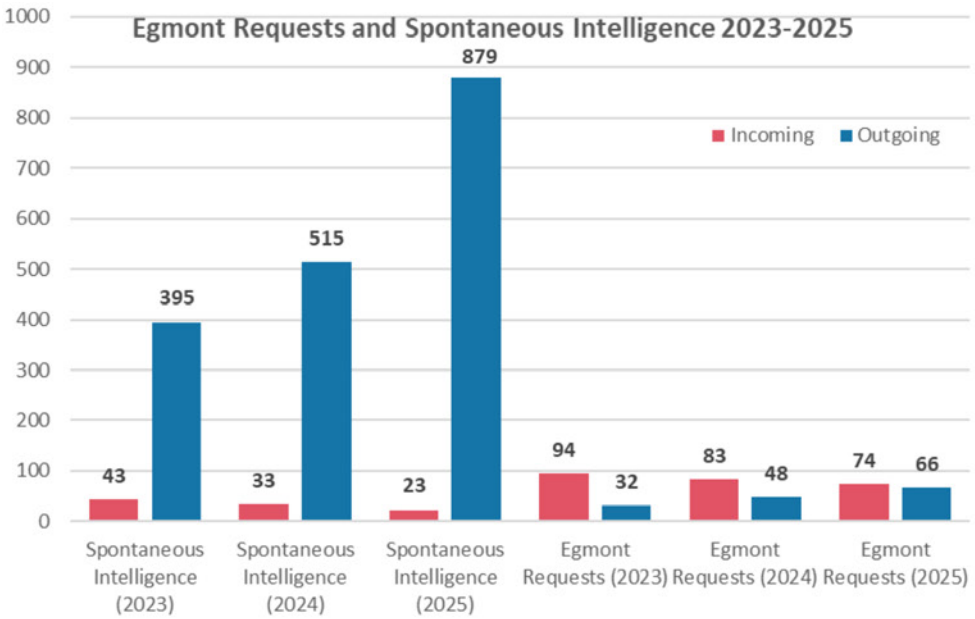
The Egmont Group of Financial Intelligence Units has outlined suggested response times for requests received by FIUs, highlighting the importance of timely engagement, irrespective of whether the response is affirmative or negative. While recognising that turnaround times will vary depending on the complexity and scope of the request, the recommended benchmark is a response within one month, where feasible. Additional time may be required where external databases must be queried or third party information is necessary to provide a complete and accurate reply.

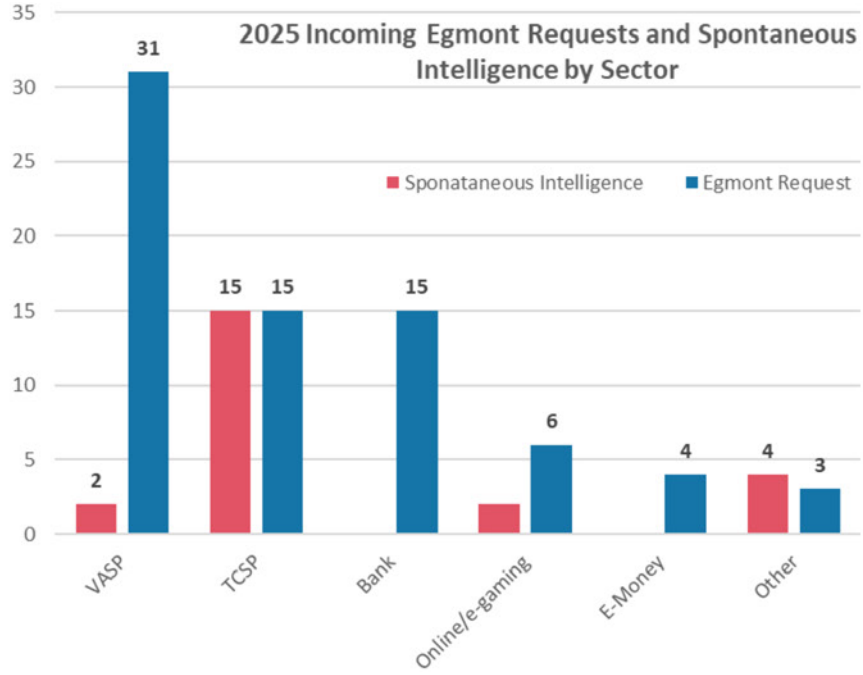
During 2025, all Egmont requests received by the GFIU required consultation with external databases and/or third parties. Notwithstanding this, 62% of requests were responded to within the recommended 30-day timeframe. Variations in response times were attributable to factors including detailed analytical review, the need for follow up enquiries, coordination with domestic law enforcement or other competent authorities, requests for clarification from the originating FIU, and the application of appropriate information-sharing risk assessments. These elements reflect the diligence, proportionality, and operational complexity inherent in managing cross-border financial intelligence exchanges.



The chart shows the timeframe for the GFIU to respond to Egmont Requests.

In 2025, the number of incoming Egmont requests decreased by 11% compared to 2024. Most of these requests relate to the VASP, TCSP and banking sectors. By contrast, outgoing Egmont requests experienced a significant rise, increasing by 38% from the previous year, continuing the trend observed in previous years.



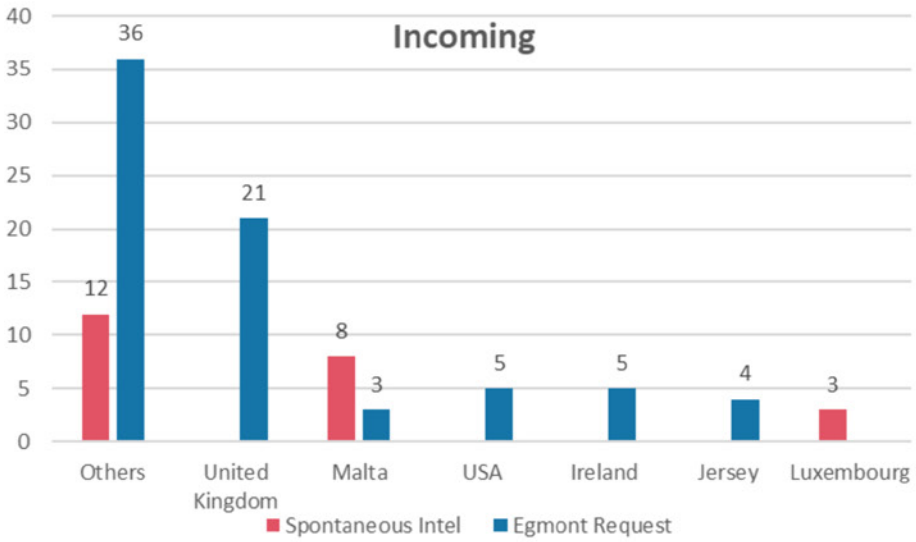


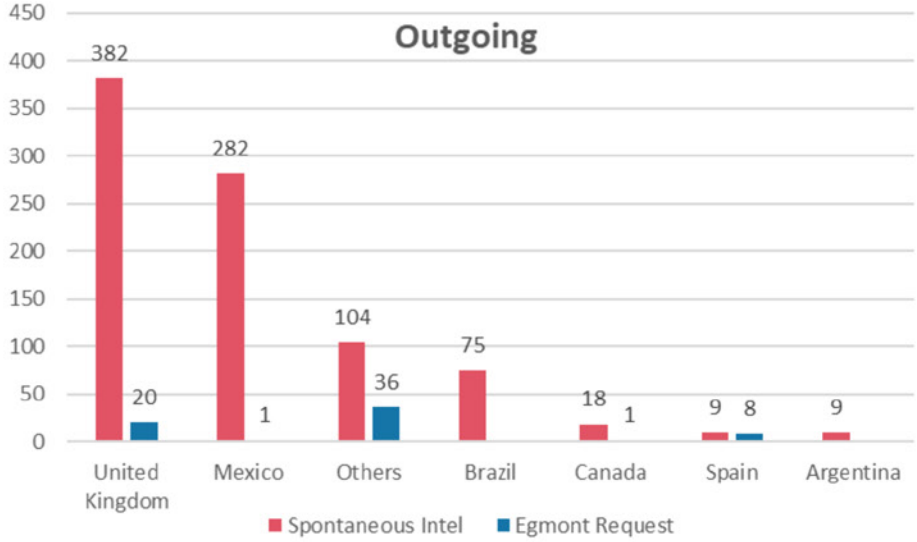
A total of 74 Egmont requests were received from 34 different jurisdictions, while 66 Egmont requests were sent to 28 jurisdictions. Additionally, 23 spontaneous intelligence reports were received from 11 jurisdictions, and 879 spontaneous intelligence reports were disseminated to 52 jurisdictions.

The spontaneous intelligence reports disseminated in 2025 relate to SARs received both in 2025 and in previous years. Reports related to SARs received in 2025 have also been disseminated in 2026. However, these are not included in the statistics presented in this report.

The UK continues to be the principal jurisdiction for Egmont engagement, with 36 incoming and 20 outgoing requests. The UK and Mexico were the top destinations for outgoing spontaneous intelligence, reflecting their positions as the top two jurisdictions cited in SARs. Whilst the UK remains the most frequently referenced jurisdiction in SARs, it is important to note that a significant number of these reports are also dual reported to the UK authorities.

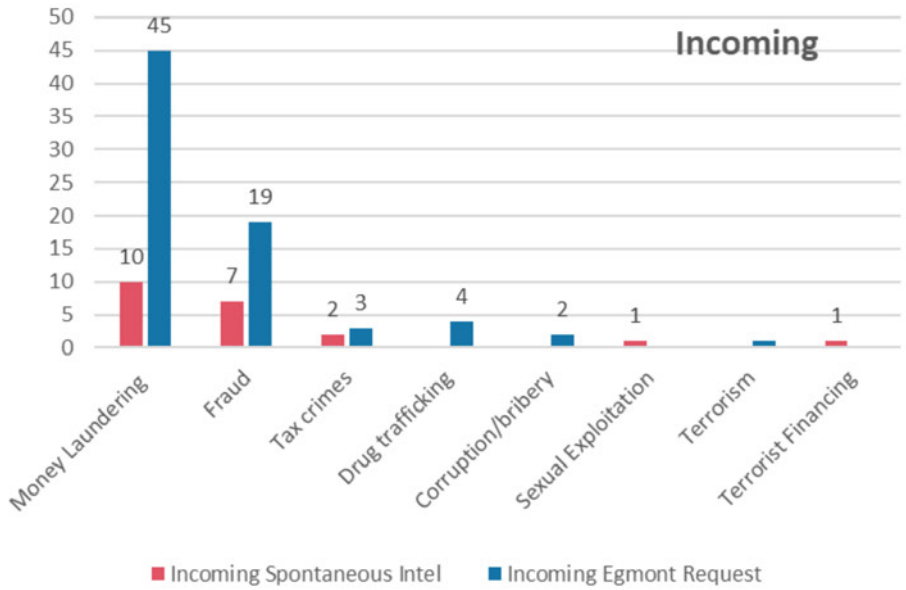
The tables below show the top jurisdictions for incoming and outgoing Egmont requests and spontaneous intelligence.

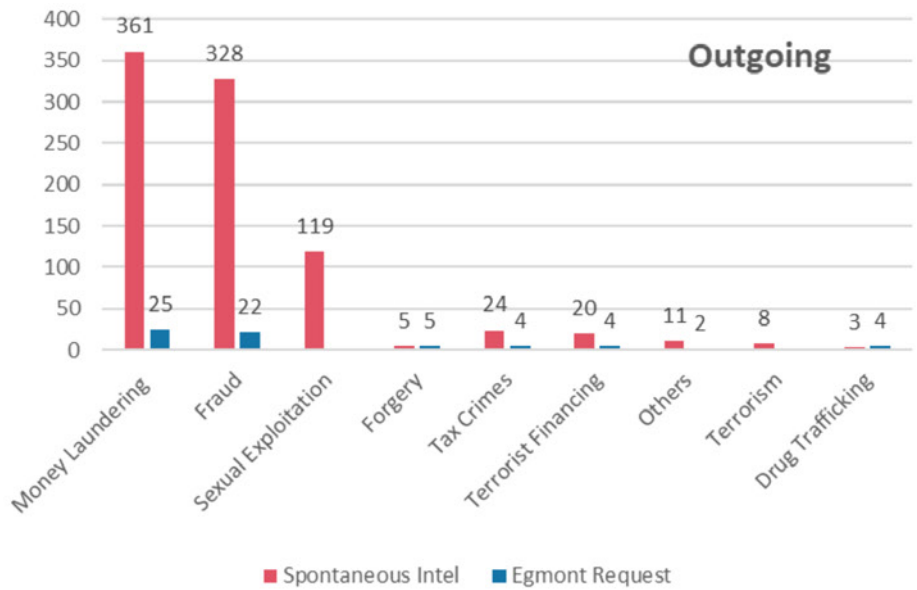




Money laundering, followed by fraud, remain the predominant suspected criminal activities associated with both incoming and outgoing Egmont requests, as well as spontaneous intelligence exchanges. As was the case in previous years, suspected sexual exploitation ranked third among the criminal activities linked to outgoing spontaneous intelligence. These cases mainly originate from SARs submitted by the VASP sector, highlighting suspected direct or indirect involvement in the distribution and receipt of child sexual abuse exploitation via the darknet.

The tables below show the top suspected criminality for incoming and outgoing Egmont requests and spontaneous intelligence for 2025.





Intelligence Reports Disseminated to Local Law Enforcement Agencies & Supervisory Bodies

The GFIU disseminates Intelligence Reports to Law Enforcement Agencies and Supervisory Bodies when considered relevant. These reports are produced based on a range of intelligence sources received by the GFIU.

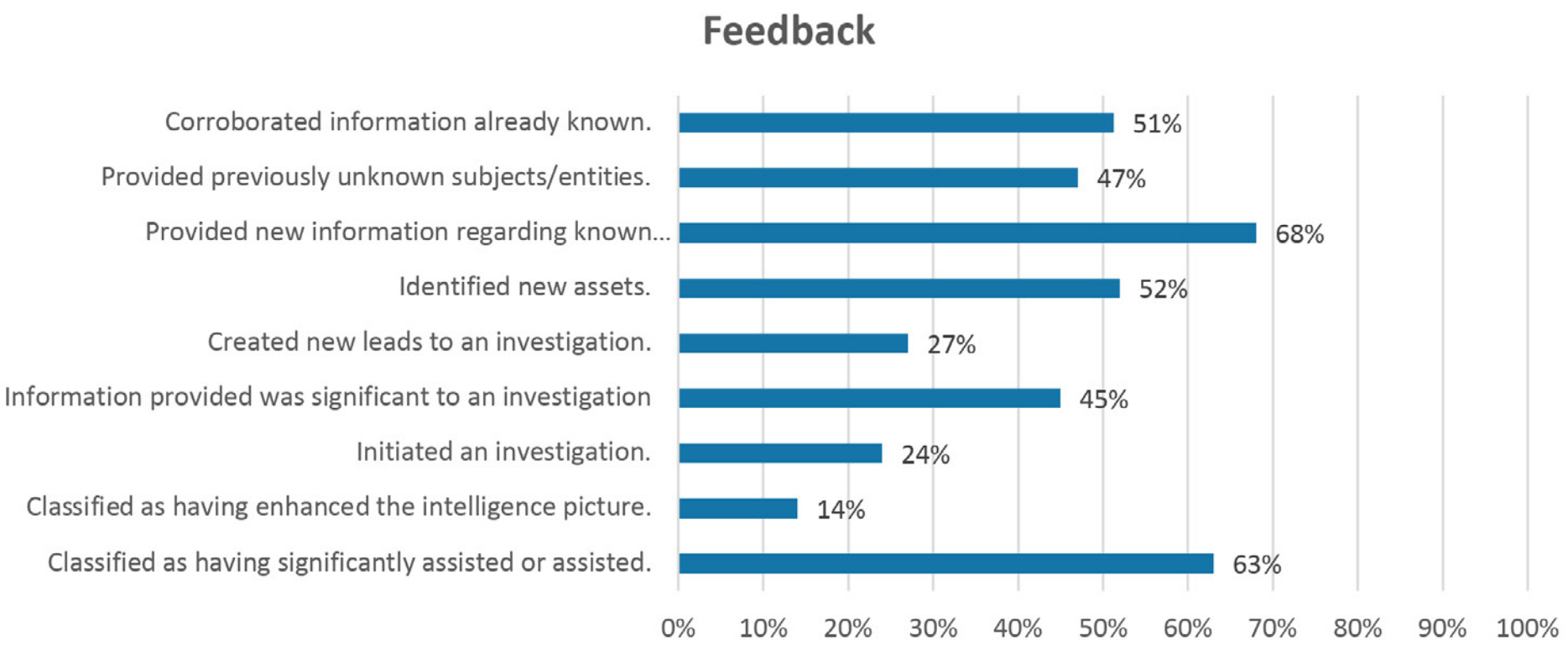
Reports disseminated rose by 154% from 142 in 2024 to 361 in 2025.

The following Intelligence Reports were disseminated during 2025.

LEA/Authority	Business Email Compromise	Corruption	Cyber-enabled Fraud	Drug trafficking	False Accounting	Forgery	Fraud	Human trafficking	Kidnapping	Money Laundering	Sanctions	Sexual exploitation	Tax Crimes	Terrorism	Terrorist Financing	Total
Sanctions Competent Authority	-	-	-	-	-	-	-	-	-	5	5	-	-	-	-	10
Department of Immigration & Home Affairs	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	1
Gambling Division	-	-	-	-	-	-	3	-	-	5	1	-	-	-	1	10
Gibraltar Financial Services Commission	-	-	-	-	2	-	1	-	-	13	1	-	-	-	-	17
HM Customs	-	1	-	2	1	-	4	-	-	13	-	-	6	-	-	27
Tax Authority	-	1	-	-	3	1	4	1	-	15	-	-	28	-	-	53
Legal Services Regulatory Authority	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-	2
Office of Fair Trading	-	-	-	-	-	-	2	-	-	1	-	-	-	-	-	3
RGP (Economic Crime Unit)	1	2	1	12	2	5	46	2	2	85	6	2	13	2	6	187
RGP (Special Branch)	-	-	-	-	-	2	-	-	-	2	2	-	1	16	28	51
Total	**1**	**4**	**1**	**14**	**8**	**8**	**60**	**3**	**2**	**142**	**15**	**2**	**48**	**18**	**35**	**361**

Feedback was received during 2025 in respect of Intelligence Reports disseminated to Law Enforcement Agencies and Supervisory Bodies. The feedback related to both Intelligence Reports disseminated during and prior to 2025.

Key highlights



Gaming Case Study 1

47 gambling accounts registered under different electronically verified identities in a 10 day period. All accounts deposited the same amount using a single virtual debit card and followed a consistent pattern of playing through the bonus funds and withdrawal behaviour.

Although all identities passed electronic verification checks, the shared payment method, uniform transaction values, coordinated activity, and structured email patterns raised suspicions of organised activity. Concerns were formed regarding potential identity misuse and possible money laundering through the use of multiple low value transactions designed to avoid detection.

Gaming Case Study 2

An online account holder registered more than 24 payment methods, including Visa cards and PayPal accounts, with over 20 identified as third party payment instruments. The individual deposited funds using both personal and third party cards and subsequently withdrew funds to third party accounts without engaging in any gambling activity.

The pattern of multiple external payment methods, immediate fund withdrawals, absence of legitimate platform use, and the customer's age profile raised significant concerns regarding potential fraud, mule activity, or money laundering. Suspicion was further heightened following receipt of a chargeback linked to one of the third party cards.

Gaming Case Study 3

Multiple customer accounts placed coordinated in play bets on low profile sporting events where odds appear unusually inflated, suggesting potential match manipulation or insider knowledge. In the observed case, a group of accounts wagered on the same obscure overseas cricket fixture, taking advantage of significantly higher in play odds compared to pre match prices. The bets generated disproportionate returns relative to the stake, with winnings withdrawn shortly afterwards.

The accounts demonstrated consistent behavioural patterns, including betting on lower tier sports markets, operating from locations with limited legitimate interest in the event, and placing wagers within similar timeframes. Internal checks also identified shared location data and other behavioural similarities linking several accounts, indicating possible coordination.

This activity aligns with known risks in the gambling sector where groups exploit potentially fixed or manipulated matches. The use of multiple accounts allows participants to distribute stakes, reduce detection risk, and obscure coordination while maximising profit. Key indicators include concentrated betting on obscure markets, abnormal odds movements, coordinated timing of wagers, and rapid withdrawal of winnings following successful bets.

VASP Case Study 1

Three newly onboarded corporate customers under common control began receiving frequent GBP payments from a single external payer shortly after account activation. The transfers occurred in tight clusters and reached volumes of roughly £75,000 per day. Immediately upon receipt, the funds were converted from GBP to EUR and then into USDT, before being sent to an external cryptocurrency wallet. That wallet rapidly dispersed the assets in smaller amounts across multiple exchanges, consistent with attempts to obscure the flow of funds.

The pattern of activity reflects red flags commonly associated with layering, use of connected or shell entities, and potential abuse of corporate vehicles to obscure the origin and destination of funds. The rapid conversion into crypto assets and subsequent dispersion across multiple platforms further aligns with typologies involving the movement of illicit proceeds through virtual asset channels

VASP Case Study 2

A VASP account was utilised to process funds originating from stolen or compromised payment card details for the purchase of cryptocurrency. The illicit funds were converted into cryptocurrency and quickly transferred to external wallets, likely to obscure the transaction trail and hinder recovery efforts by the issuing financial institutions.

The use of multiple payment cards, accounts, and rapid withdrawals is indicative of attempts to distance the funds from the original fraudulent activity and to facilitate further laundering through subsequent transfers across wallets or cryptocurrency exchanges

Bank Case Study 1

A victim reported being the subject of a social media rental scam. The victim had identified a holiday property advertised on Facebook, with communications subsequently moved to WhatsApp. The suspected fraudster provided photographs, an address, and a fraudulent contract to support the legitimacy of the rental.

The victim made an initial deposit followed by a further payment for the balance shortly before the planned trip. Upon arrival at the provided address, the customer discovered that the property did not exist.

Bank Case Study 2

A customer exhibited behaviour consistent with the misuse of his personal bank account to move funds rapidly through the financial system. The account showed frequent cash deposits, often in close succession and without an identifiable rationale. In parallel, the customer received multiple transfers from unrelated third parties, with no clear explanation of the underlying purpose or relationship between the parties involved.

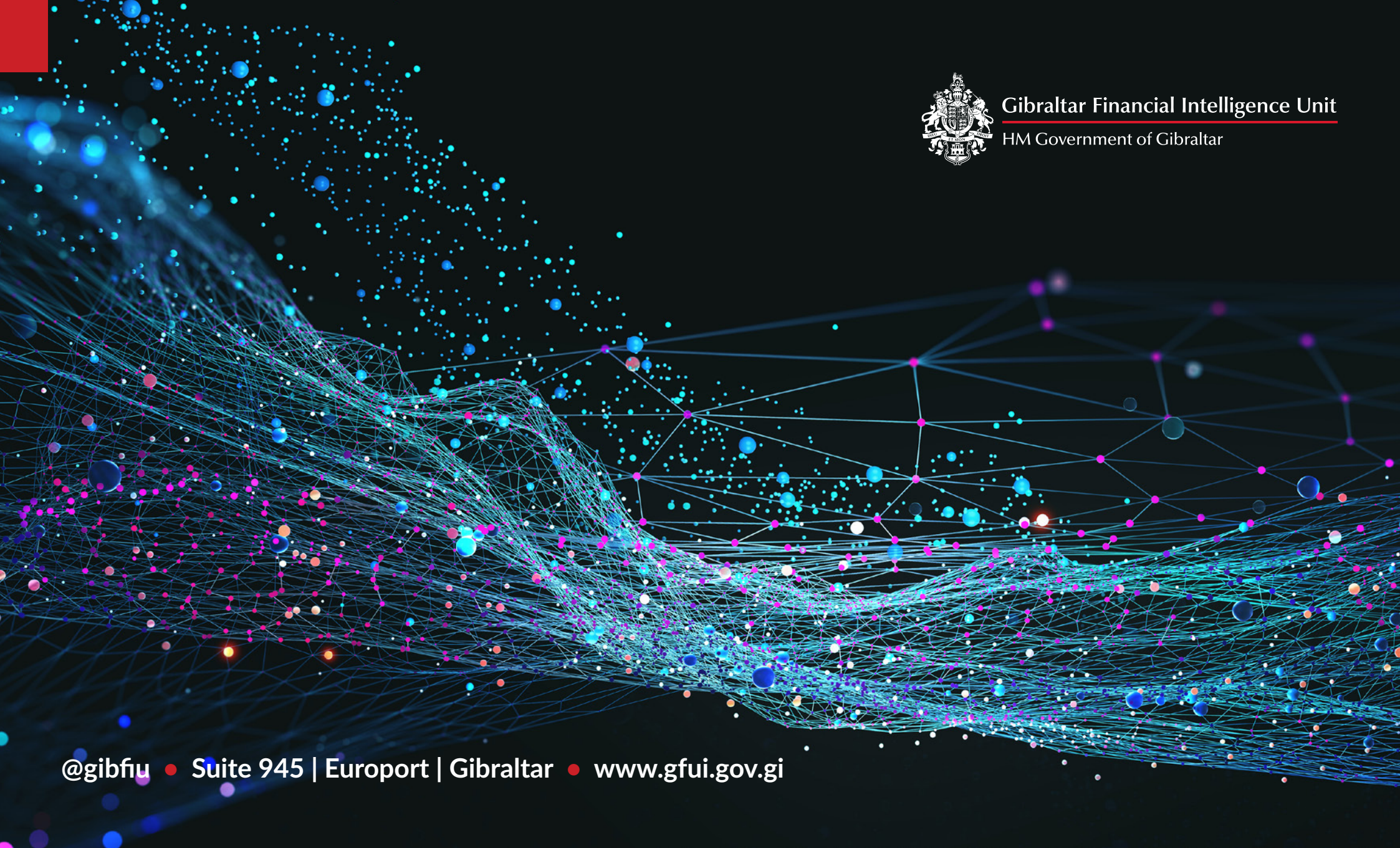
Once funds were credited, whether from cash deposits or incoming transfers, they were immediately sent onward to accounts held with various challenger banks. The rapid movement of funds, combined with the absence of legitimate economic activity, suggests the account may have been used to obscure the origin and destination of money.

TCSP – Case Study 1

A company entered into multiple consultancy contracts, made regular payments, and recorded the costs as legitimate expenses. However, there was no evidence that any consultancy work was actually performed, and several consultants had no relevant expertise or were closely connected to the business. This pattern suggests the agreements may have been used to extract funds, disguise payments, or create artificial expenses for tax purposes.

e-Money Case Study 1

A newly opened personal payment account displayed activity consistent with authorised push payment fraud shortly after on-boarding. The account holder received multiple incoming transfers that were later linked to external fraud reports submitted by remitting banks. In each case, victims believed they were purchasing event tickets advertised through social media. After sending the funds, the victims reported that the seller stopped responding and no goods were delivered.


Gibraltar Financial Intelligence Unit
HM Government of Gibraltar
@gibfiu • Suite 945 | Europort | Gibraltar • www.gfui.gov.gi