



# ANNUAL REPORT 2024

## & 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.

Please click [here](#) to share your thoughts.

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

**3**

Director's Message



**5**

Our Organisation



**7**

Our People



**10**

Our Technology



**12**

Our Strategy



**14**

Our Outreach



**17**

Our International Work  
(Egmont/ Quad/ IACCC)



**20**

Our Partnerships



**23**

Our Achievements



**25**

Strategic Analysis Report





**Edgar Lopez**  
**Director, GFIU**

I am pleased to present the Gibraltar Financial Intelligence Unit's Annual Report for 2024. This report reflects not only the significant strides we have made in our fight against financial crime, but also our commitment to implementing the 2023-2026 strategy in the face of a dynamic and increasingly complex threat landscape. The evolving nature of financial crime demands agility, innovation, and resilience, qualities which the GFIU team continues to demonstrate with exceptional dedication and professionalism.

A key milestone during the year was the approval of our 2024 business case, which facilitated a substantial expansion of our team. Within six months, we successfully doubled our human resources, introducing several strategic roles, including Intelligence Managers, that have greatly enhanced our analytical capabilities and operational resilience. This growth has strengthened our ability to detect and respond to emerging financial crime typologies with greater precision and efficiency.

Our collaboration with key stakeholders has also deepened. The integration of a Tax Officer within the GFIU has significantly enhanced the fusion of financial intelligence and tax data, contributing to a more coordinated response to illicit finance and tax crimes. While the pace of growth has presented challenges, particularly in delivering specialist training, it has also opened new opportunities to build a more capable and future-ready unit. We have expanded our training programmes and capacity-building initiatives, ensuring our officers are trained to tackle the challenges ahead.

Innovation remains at the heart of our work. In 2024, we invested in advanced open-source intelligence (OSINT) software, further improving our capacity to harness information from publicly available sources. These tools have enhanced both the speed and depth of our intelligence analysis, reinforcing our ability to deliver timely and actionable insights.

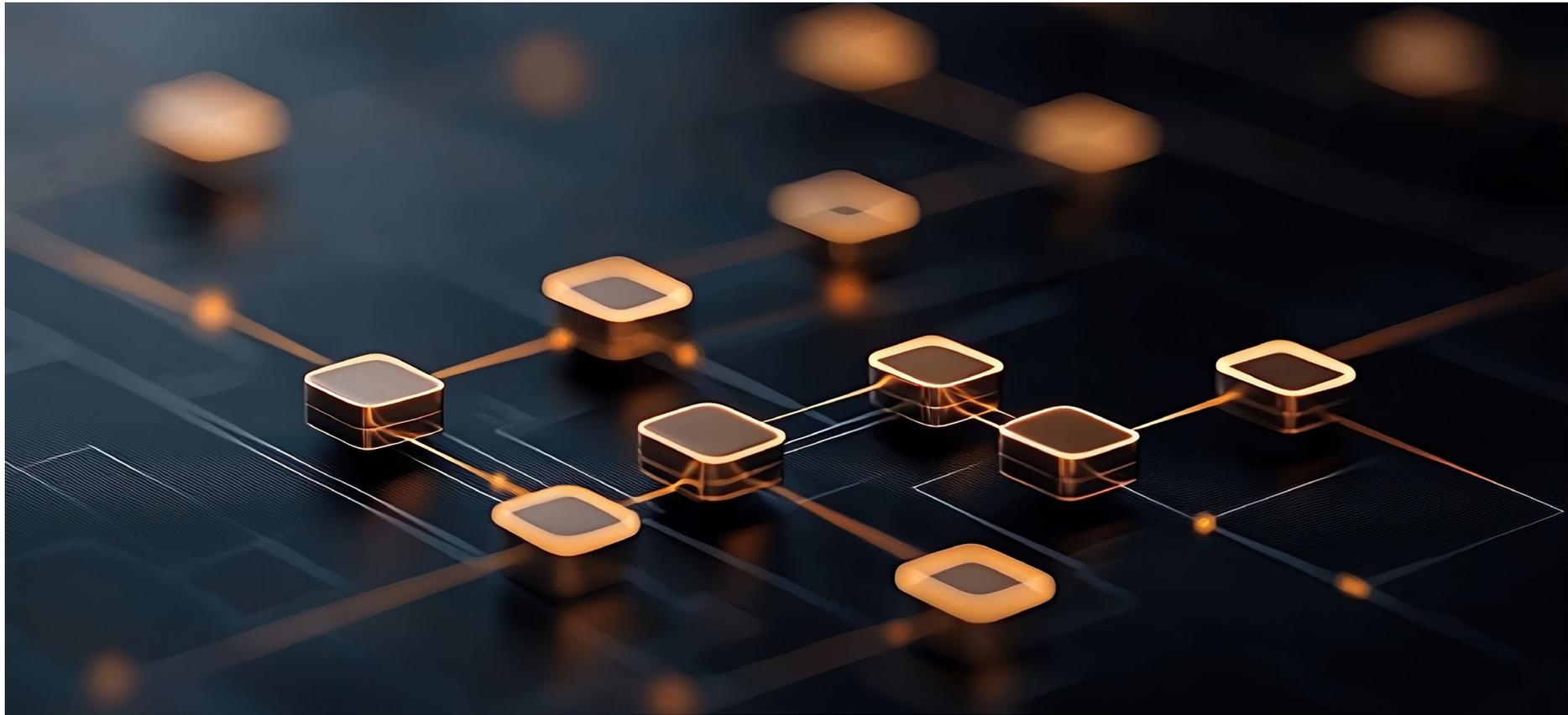




Our outreach efforts through Project Nexus continue to play a central role in strengthening engagement with both public and private sector entities. Through engagement clinics and targeted initiatives, we have seen marked improvements in the quality of Suspicious Activity Reports (SARs), reflecting greater awareness and collaboration across reporting entities. Internationally, the GFU has strengthened its presence through active participation in the Egmont Group, Europol's Financial Intelligence Public Private Partnership, and the Quad Forum. Our contributions in these groups highlight Gibraltar's role as a committed and credible voice in the global financial intelligence community.

The progress outlined in this report would not have been possible without the dedication of our staff. Their commitment, professionalism, and adaptability have laid the foundation for continued success and further growth. As we look ahead to the future, I remain confident that the GFU will continue to evolve, adapt, and lead in our collective mission to combat financial crime.





# 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, 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 has had a distinguished career serving as a police officer in the Royal Gibraltar Police, primarily working in specialist departments within the Crime and Protective Services Division. He was the Head of Special Branch before becoming the Head of Interpol Gibraltar Sub-Bureau, gaining experience in criminal and counter-terrorism intelligence. Edgar holds a Master's degree in International Affairs specialising in Cybersecurity at King's College London. His dissertation focused on the use of the cyber domain by state actors to fund illicit nuclear weapons and missile programs. With experience in the MONEYVAL and Financial Action Task Force (FATF) processes, Edgar brings a wealth of knowledge in the FATF Recommendations and Standards.

He remains focused on tackling proceeds of crime specifically centred on victim-based crime such as Human Trafficking, Cyber-enabled Fraud and Online Child Sexual Abuse and Exploitation. He also provides technical and specialist assistance to other jurisdictions in implementing frameworks to counter proliferation financing and in establishing effective public-private partnerships. This advisory role reinforces international cooperation efforts and places Gibraltar firmly on the map as a leader in financial intelligence and the global fight against financial crime.



## Head of Operations

Carl Ramage joined the GFU as Head of Operations in December 2021. Called to the Bar of England and Wales (and Gibraltar) in 2007, Carl brings over 15 years of Criminal Justice experience. In 2013, he was appointed Crown Counsel for HM Government of Gibraltar, spending eight years at the Office of Criminal Prosecutions and Litigation (OCPL).

During his time at OCPL, Carl was involved in some of Gibraltar's most significant trials, including cases of murder, rape, serious sexual assaults, and offences against children. He also underwent specialist training in Rape and Serious Sexual Offences with the Crown Prosecution Service in the UK. His prosecutorial work has extended to financial crime, including fraud and false accounting, with several cases resulting in the confiscation of criminal proceeds.

In the past year, Carl has continued to strengthen his expertise in economic crime and financial intelligence. He has participated in a range of professional development programmes, including the commencement of a global sanctions specialist course, and continues to actively engage with the private sector through Project Nexus events. Carl remains a key contributor to the GFU's outreach initiatives, regularly delivering at engagement clinics and industry events.



## Our Team

The GFU's operational framework, structured around International, Domestic, and Analysis Desks, creates a more responsive and adaptable approach to financial intelligence. In early 2024, a new business case was approved, resulting in a near doubling of our team. This expansion included the introduction of new managerial roles, with Intelligence Managers now playing a pivotal role in overseeing operational functions. Their leadership enables senior management to dedicate greater focus to strategic initiatives.

Furthermore, we have strengthened our resilience within the International and Analysis Desks, enhancing capacity across key areas of responsibility. The Analysis Desk plays a pivotal role by providing critical support to the entire team. Our Financial Intelligence Officers (FIOs) collaborate closely with our Analysts, supported by our Financial Intelligence Support Officers. Their diverse skill set complements a modern working environment that amplifies the GFU's pursuit of its objectives.

We prioritise inclusivity and diversity in our workplace, aiming to empower staff members to reach their full potential and contribute to the GFU's performance. By bringing together a wide range of skills, knowledge, and experiences, we enhance productivity, decision-making, and problem-solving capabilities. All our staff undertake

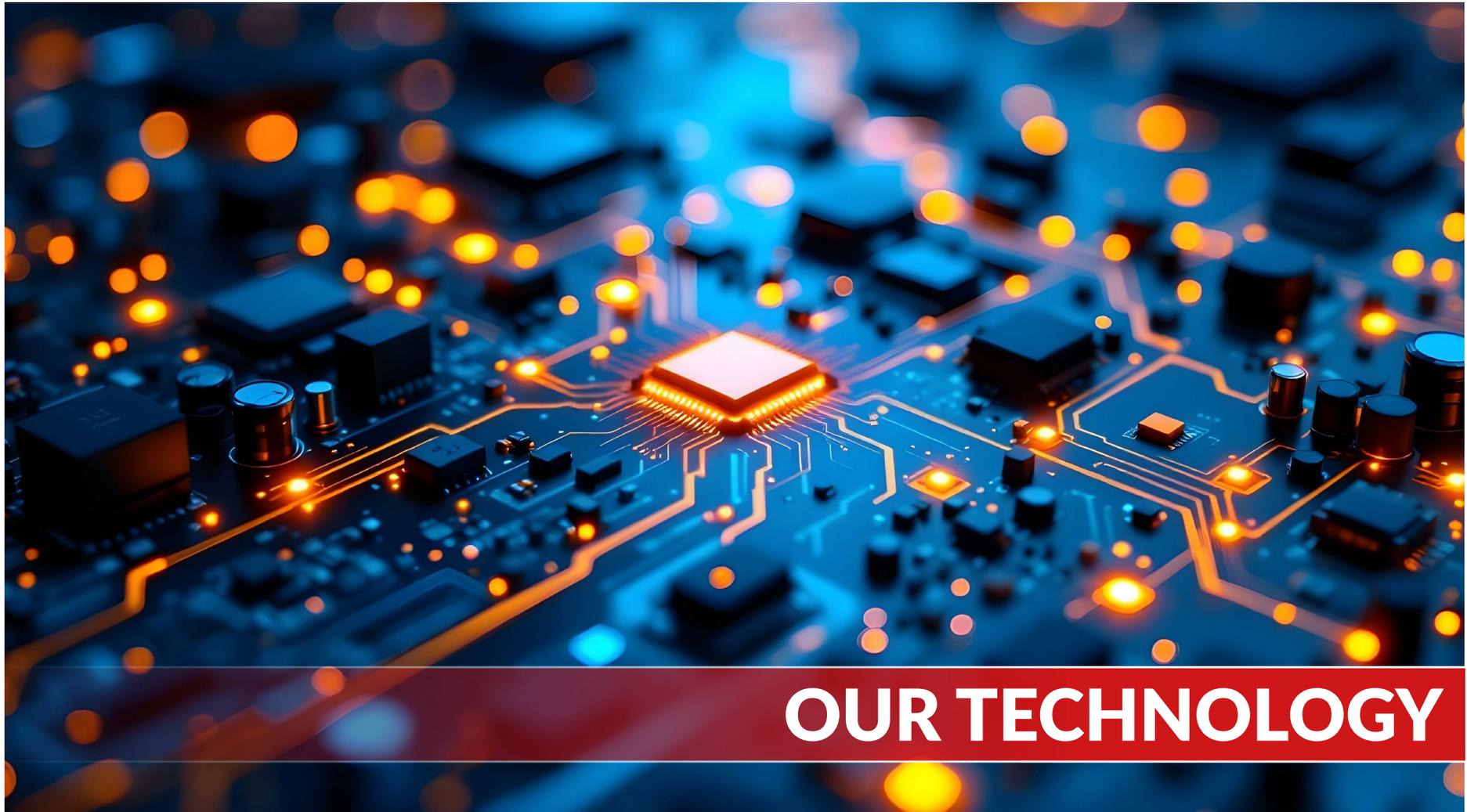




in-house training and mentoring programmes, followed by a FIO course with the UK's Proceeds of Crimes Centre (the body that accredits and monitors the performance of all financial investigators in England, Wales and Northern Ireland).

We have established a culture that values diverse perspectives and embraces difference. This supports a positive and healthy work environment where individuals feel empowered to make choices, fostering innovation and productivity. This approach is reinforced by effective leadership and management practices, all of which are aligned with our 3-year Strategic Plan. Training is an integral aspect of the GFIU's mandate, ensuring the maintenance of core skills. We regularly conduct in-house training sessions and utilize e-learning courses from various providers, including Egmont's ECOFEL and Interpol's "I-Le@rn" systems, to stay updated with a changing threat environment.





# OUR TECHNOLOGY



THEMIS is the GFIU's primary IT case management system, facilitating the secure submission of SARs. Continuous upgrades have refined it into an adaptable platform that evolves with the GFIU's digital transformation. Designed with a modular framework, THEMIS enhances interoperability, resilience, and security.

Featuring an online portal for Money Laundering Reporting Officers (MLROs) and a secure access system for the GFIU, law enforcement agencies (LEAs), and Government Law Offices, THEMIS streamlines SAR submissions. It allows for detailed data entry while maintaining flexibility for reports with limited information. The internal system enables seamless communication with reporting entities, facilitating additional information requests and the secure distribution of official notices and updates.

Ongoing enhancements have expanded THEMIS into a centralised repository for financial intelligence, encompassing international requests, spontaneous disclosures, Mutual Legal Assistance (MLA) requests, law enforcement notifications, sanctions monitoring, and intelligence analysis. A visual data dashboard integrated with THEMIS improves analytical capabilities, proving invaluable for strategic analysis and intelligence management. The GFIU continues to explore artificial intelligence (AI) into its systems to enhance money laundering and terrorist financing detection. These advancements will drive improved accuracy, efficiency, and proactive financial crime identification.

In addition to these developments, the GFIU uses advanced cryptocurrency tracing tools to monitor and analyse transactions conducted on public blockchains. These tools enable investigators to follow the flow of funds across crypto wallets and exchanges, identify clustering patterns, and detect links to known threat actors. By visualising transaction pathways and overlaying them with attribution data from exchanges and other databases, the GFIU can trace proceeds of crime, monitor typologies, and support timely intervention

by law enforcement. This capability is crucial in addressing the increasing exploitation of virtual assets for money laundering, terrorist financing, and other predicate offences.

To further enhance financial intelligence products, the GFIU also integrates Open Source Intelligence (OSINT) tools into its analytical processes. These tools allow analysts to gather relevant publicly available data from media, social networks, corporate registries, and the internet. OSINT supports the identification of connections between subjects of interest, geographic risk indicators, and reputational concerns, helping to build comprehensive intelligence reports. When combined with SAR data and blockchain analytics, OSINT provides contextual depth and can reveal behavioural patterns or associations not immediately evident through traditional financial sources alone. This layered approach strengthens the GFIU's capacity to produce actionable intelligence for investigation and enforcement.





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.







# PROJECTNEXUS

Project Nexus was conceived to bridge the gap between the public and private sectors in the fight against financial crime. Its name signifies the interconnectedness required for a collaborative approach to intelligence-sharing and awareness.

This award-winning initiative engages reporting entities mandated to submit SARs, fostering an environment where financial institutions and regulatory bodies align efforts. By facilitating structured engagement, Project Nexus supports operational best practices, promotes awareness of financial crime trends, and ensures reporting entities stay informed about legislative updates and evolving criminal tactics.

The initiative has yielded measurable improvements in SAR quality, with the introduction of Project Nexus Engagement Clinics proving instrumental. These clinics provide targeted training for professionals, equipping them with practical skills to identify and report suspicious activity more effectively.

Aligned with the GFIU's Corporate Communication Strategy, Project Nexus leverages multiple engagement channels to maximize outreach impact.

Recent participant feedback has underscored its success, with 100% of respondents rating engagement events as excellent or good.

A new document, **Project Nexus Information 2024**, has been created to provide a comprehensive overview of the initiative's outreach and engagement processes. Designed as an accessible resource for both new and existing stakeholders, the document clearly outlines the objectives, methods, and benefits of participation in Project Nexus. It serves as a practical guide for reporting entities, detailing how structured engagement activities, such as clinics, events, and targeted communications, contribute to enhanced collaboration and capacity building. This publication reinforces the initiative's commitment to transparency, consistency, and continued support for stakeholders in meeting their reporting obligations.



## The three-phases of Project Nexus



To enhance the good rapport established over the years between the industry and key partners, which had been improved by the support from the Gibraltar Association of Compliance Officers.

To ensure that the subjects in the program of events covered the most relevant and current information available, delivered through a forecast of regular events.

To develop a means of delivering training through the use of technology.



The e-Nexus Series is an online learning platform designed to enhance awareness among financial and non-financial reporting entities. Offering interactive workshops and training modules, e-Nexus covers topics such as legislative updates, emerging financial crime typologies, and international compliance obligations.

With over 600 registered users, e-Nexus provides flexible access to essential resources, ensuring professionals stay ahead of evolving threats. Recent user feedback has been overwhelmingly positive, with 97% rating workshop quality as excellent or good.





# OUR INTERNATIONAL WORK





The Egmont Group facilitates and prompts the exchange of information, knowledge and co-operation between member FIUs in their common fight against financial crime. As a member since 2004, the GFIU actively exchanges intelligence with international FIUs. In 2024, it participated in the Egmont Working and Regional Group meetings in Malta and attended the 30th Annual Egmont Plenary in Paris. These meetings enable global collaboration, ensuring the GFIU remains at the forefront of financial intelligence-sharing. As part of the Europe II Group, the GFIU has participated as a co-lead in a new project focussing on a horizontal review of FATF IO2, IO6 and Recommendations 29 and 40.



The GFIU became an Associate Member of the IACCC in 2020, strengthening its ability to support international corruption investigations. Hosted by the National Crime Agency in London, the IACCC allows FIUs and law enforcement agencies from smaller financial centres to rapidly exchange intelligence with the IACCC and assist with the development of the intelligence picture on grand corruption cases. Made up of nine law enforcement agencies from Australia, Canada, New Zealand, the UK, USA, and Singapore, the IACCC can provide further support to partners across the world with grand corruption investigations, including the facilitation of Mutual Legal Assistance (MLA) requests between their jurisdictions. With a dedicated liaison officer, the GFIU facilitates intelligence-sharing on grand corruption cases and benefits from specialised training in areas such as bribery, cryptocurrency investigations, and open-source intelligence.

In April 2024, the GFIU attended a meeting at INTERPOL's Global Complex for Innovation in Singapore, which serves as INTERPOL's headquarters for cyber-related matters. This meeting brought together key partners of the IACCC to discuss emerging threats at the intersection of grand corruption and cyber-enabled crime. The meeting provided an opportunity to strengthen international partnerships, share best practices, and explore technological innovations to enhance the global response to corruption. It also reinforced the GFIU's commitment to remaining at the forefront of international collaboration through active participation in initiatives related to training and guidance.





The GFIU collaborates closely with FIUs from Guernsey, the Isle of Man, and Jersey through the Quad Forum. This partnership promotes best practice sharing, joint training, and enhanced cooperation with law enforcement agencies. In 2024, the Quad Forum facilitated a course on terrorist financing in Gibraltar House, London with the UK's National Terrorist Financing Intelligence Unit.

Throughout 2024, the Quad Forum has worked closely on a comparative analysis to examine both the commonalities and differences that define our jurisdictions. This exercise has not only deepened our understanding of each member's operational context but also strengthened our collective identity. By identifying where we align and where we diverge, the result of the analysis is helping to shape the future direction of the Quad Forum. It

provides a strategic foundation for how we, as a strategic collective, can better understand and respond to the evolving threats we face. Rooted in a shared commitment to international cooperation and underpinned by similar values, structures, and challenges, this work enhances our ability to mitigate transnational crime more effectively and positions the Quad Forum as a collaborative force in the global fight against financial crime.





# OUR PARTNERSHIPS





The Financial Liaison and Intelligence Network (FLINT) fosters collaboration between law enforcement, regulators, and the financial sector in Gibraltar. Established in 2022, it enables strategic intelligence-sharing, risk identification specific to Gibraltar, and the development of financial crime typologies.

FLINT embraces the expertise and resources of public sector bodies responsible for combating money laundering, terrorist financing, and proliferation financing, together with industry experts from the banking sector. By bringing together stakeholders across the private and public sector, FLINT seeks to identify and mitigate emerging and persistent risks through strategic and operational intelligence. It facilitates the development of sector-specific typologies on evolving criminal trends and offers informed analysis for future National Risk Assessments. Enhanced information sharing among law enforcement entities in Gibraltar enables a deeper understanding of specific risks and vulnerabilities.

Through the establishment of FLINT and our membership of the Quad Forum we have been able to align ourselves with the UK's Joint Money Laundering Intelligence Task Force (JMLIT+), further enhancing our intelligence capabilities. We have subsequently participated in the Europol Financial Intelligence Public Private Partnership (EFIPPP) to broaden our collaborative efforts in combating money laundering, terrorism financing, and proliferation financing on a global scale.





## Royal United Services Institute – Centre For Financial Crime & Security Studies

Since 2023 the GFIU has been partnered with the Centre for Finance and Security (CFS) at RUSI, a leading security think tank based in Whitehall, London. Founded in 2014, the CFS aims to challenge the status quo and build resilience in the global response to illicit finance, producing a broad range of research publications. This collaboration enhances research, policy development, and capacity-building initiatives in financial crime prevention.

During 2024, the GFIU has participated in several conferences and initiatives hosted by RUSI, including the Maritime Sanctions Taskforce and UK Sanctions Implementation and Strategy Taskforce, which ensures the GFIU is involved in and can contribute to key international debates on financial crime and security.

## CIFAS

In 2023, the GFIU joined Cifas, the UK's fraud prevention network, reinforcing efforts to combat economic crime. Membership in Cifas strengthens intelligence-sharing and aligns the GFIU with global best practices in fraud prevention.

The GFIU remains committed to adapting to emerging threats, strengthening partnerships, and using technology to protect Gibraltar's financial system. Through strategic collaboration and innovation, it continues to enhance its role in global financial intelligence.





# OUR ACHIEVEMENTS



Throughout 2024, the GFIU has made significant strides in enhancing its operational capabilities, strengthening international cooperation, and engagement with both public and private sector stakeholders. These achievements reflect the Unit's proactive approach and commitment to tackling financial crime in all its forms.

- Launched a new e-Nexus workshop on the Money Mule Schemes
- Conducted numerous strategic level meetings with the Financial Liaison & Intelligence Network (FLINT) public private partnership
- Attended various Europol Financial Intelligence Public Private Partnership (EFIPPP) meetings and participated in several projects and workstreams
- Delivered a Masterclass on SAR Writing in association with the Gibraltar Association of Compliance Officers
- Delivered a training session with the gaming sector in association with the Gibraltar Betting and Gaming Association
- Attended a Small States and Territories Working Group meeting in Monaco co-leading on a proliferation financing project
- Attended various meetings with the Quad Forum of FIUs and conducted a comparative analysis with Jersey, Guernsey and the Isle of Man
- Delivered Project Nexus events throughout the year to continue making improvements to the quality of the suspicious activity reports
- Presented at the Anti Money Laundering Group of the UK Gaming and Betting Council, in London providing the audience with valuable insights into the current and residual trends and typologies in financial crime in the Gaming sector
- Presented in the '2024 International Forum on Police Cooperation - Combating Transnational Fraud' with a contribution on the new trends in crypto crime session, focusing on the abuse of the cyberspace to conduct sophisticated virtual asset-related crime on crypto exchanges
- Delivered training for the Council of Europe's Partnership for Good Governance programme for the Eastern Partnership countries on establishing Public-Private Partnerships
- Hosted United States special agents and experts in crypto investigations for a seminar on cyber enabled crime, including experts from Asset Reality in asset recovery techniques
- Represented Gibraltar in the FCDO's, "Illicit Financing Dialogue" meetings, hosted in Miami, USA
- Completed a Terrorist Financing Course in London (Gibraltar House) with the Quad Forum in collaboration with the UK's National Terrorist Financing Intelligence Unit (NTFIU)
- Increased the GFIU's human resources and invested in advanced technologies in our efforts to combat economic crime
- Attended the 24th Annual Egmont Working and Regional Groups Meetings in Malta and the 30th Egmont Group Plenary in Paris, France.





## Strategic Analysis Overview

In recent years, the GFIU has undertaken a range of initiatives aimed at enhancing the quality and utility of its strategic analysis outputs. Among these efforts was the implementation of targeted surveys to assess the effectiveness of its analytical products. This report represents the integration of financial intelligence with a structured strategic analysis framework, designed to provide professionals and stakeholders with deeper insights into money laundering (ML), terrorist financing (TF), and proliferation financing (PF) trends and patterns specific to Gibraltar.

Drawing on multiple sources and methodologies, this report seeks to achieve the following objectives:

- Collating annual data to identify patterns and recurring concepts within the financial landscape.
- Collecting, assessing, and organising additional information from other competent authorities, as necessary, to enhance the findings and insights.
- Identifying connections or links between various pieces of information to uncover hidden relationships and potential trends within the data.

The strategic analysis presented herein highlights key money laundering threats and vulnerabilities, drawing from SARs submitted by Gibraltar based

reporting entities and supported by additional intelligence sources.

Informed by a review of previous quarterly statistical publications, the GFIU has refined its reporting methodology by excluding SARs filed solely under the Sanctions Act. Going forward, the scope of analysis will be limited to reports submitted pursuant to the Proceeds of Crime Act 2015 and the Terrorism Act 2019. This adjustment enhances analytical consistency and ensures that findings are more directly aligned with the typologies and trends related to money laundering, terrorist financing, and related predicate offences.

To maintain consistency with Financial Action Task Force (FATF) terminology, the Distributed Ledger Technology (DLT) sector is now categorised under the Virtual Asset Service Provider (VASP) designation within this report.

In 2024, the volume of SARs received increased by 1.7% compared to 2023. While overall reporting levels remained relatively stable, a notable reduction in submissions from the gaming sector was observed. This decline was counterbalanced by a near twofold increase in SARs submitted by the VASP sector over the same period.

As in previous years, money laundering and fraud

were the most commonly suspected offences identified in SARs. In particular, there was a marked rise in fraud related submissions from the VASP, gaming, and banking sectors. These reports frequently involved payment fraud, investment scams, and Ponzi schemes.

Reports involving suspected sexual exploitation, particularly from the VASP sector also continued to increase. These cases often included indicators of both direct and indirect involvement with child sexual abuse material, often circulated via the darknet.

Tax related SARs also saw an upward trend, with many involving undeclared income. A significant proportion of these submissions related to individuals lacking a direct nexus to Gibraltar.

Know Your Customer (KYC) concerns, adverse media, and open source intelligence continued to be key grounds cited in support of suspicions underpinning SAR submissions.

SARs received in 2024 were connected to 100 jurisdictions, with the United Kingdom remaining the most frequently cited nexus. The UK also accounted for the highest volume of both incoming and outgoing Egmont requests.





A total of 2,340 SARs were dual disclosed in 2024, representing 47% of all submissions, down from 3,098 SARs (63%) in 2023. The majority of these dual disclosures originated from the gaming sector and involved cases with a UK nexus.

Of the SARs assessed for quality, 98% were deemed to meet the GFIU's standards, while only 0.7% were identified as defensive in nature.

Consent requests increased by 28% year on year, with 406 received in 2024.

The number of spontaneous intelligence reports disseminated to foreign jurisdictions rose by 30%, with Mexico and Brazil emerging as the principal recipient countries.

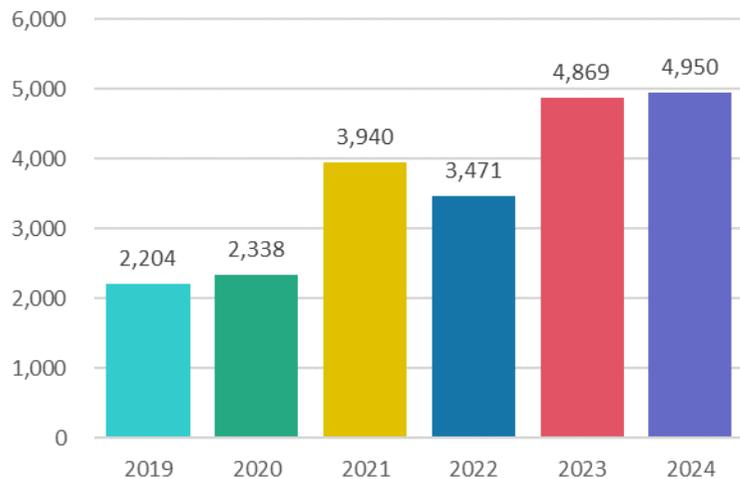
Domestically, 142 intelligence reports were shared with Gibraltar's law enforcement agencies and supervisory bodies—an 8% increase compared to the previous year.

In 2024, the number of incoming Egmont requests declined by 12% compared to 2023. Most of these requests, along with spontaneous intelligence received, were linked to the TCSP, VASP, and banking sectors. The predominant suspected offences involved money laundering, fraud, and tax related crimes.

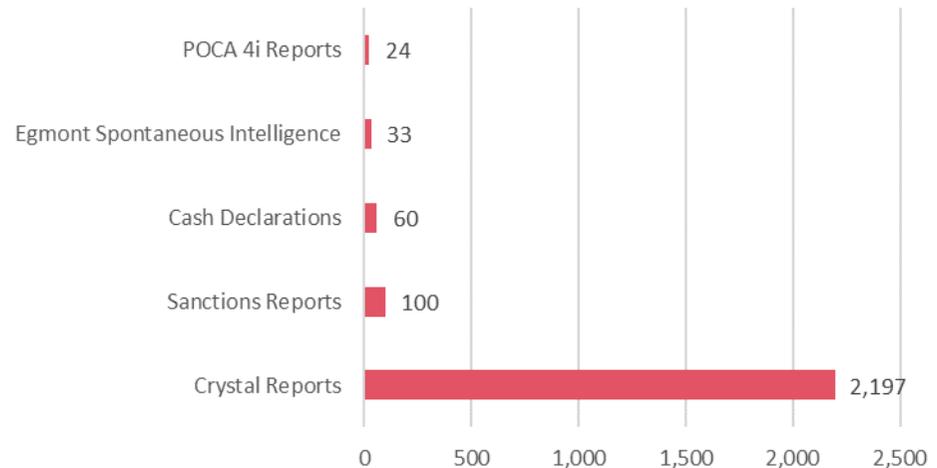


Unless otherwise stated, the statistics in this report relate to the year 2024 and are presented in comparison to 2023. The data has been extracted from our reporting system, Themis, and analysed using dedicated analytical software. It is important to note that Themis is a live database; therefore, the figures provided represent a snapshot in time. While discrepancies between this and other GFIU publications should be minimal, minor variations may occur due to system updates or the inclusion of additional information.

### SARs received by the GFIU



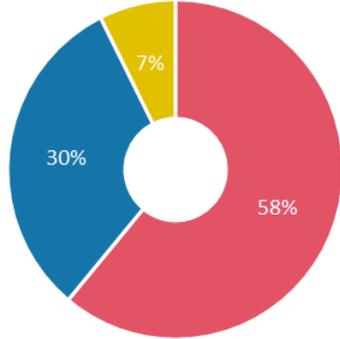
### 2024 Other Intelligence Sources



Crystal Reports are received from the UKFIU and serve as valuable data matching reports that enhance the intelligence capabilities of the GFIU. These reports compare and align information across multiple datasets to identify potential links or matches involving Gibraltar based persons or entities, or any nexus associated with Gibraltar. Each report undergoes a process of operational analysis, following a methodology very similar to that applied to SARs. The GFIU places a high value on these reports, recognising them as a key source of intelligence that supports its strategic and operational objectives. This valuable intelligence sharing initiative has been made possible through the strong and ongoing collaboration between the GFIU and the UKFIU.

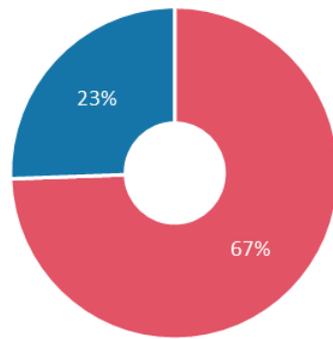


Reporting Sectors



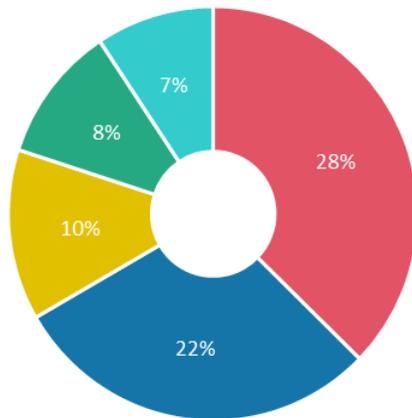
■ Online/e-Gaming ■ VASP ■ Bank

Suspected Criminality

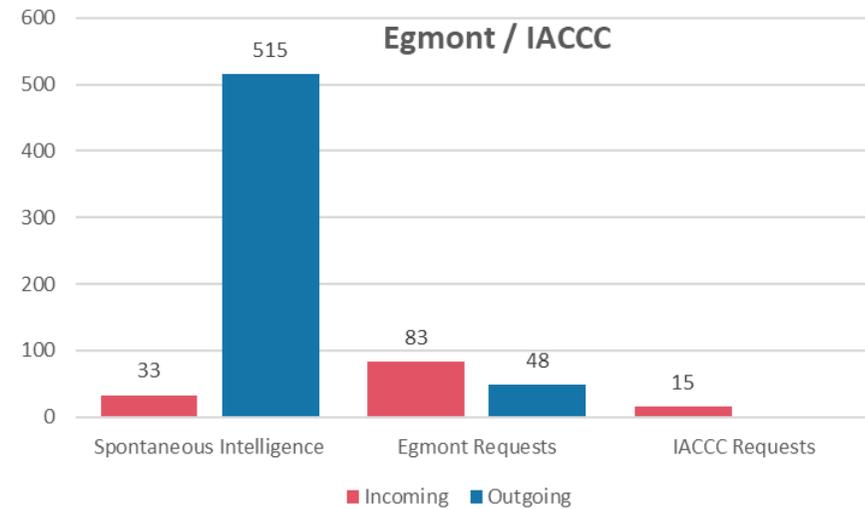
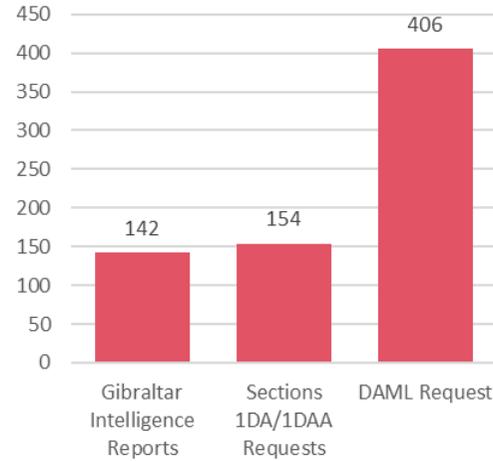


■ Money Laundering ■ Fraud

Grounds for Suspicion



■ KYC related issues  
 ■ Adverse open source  
 ■ Fraud, forgery and false accounting  
 ■ Dark Web Exposure  
 ■ Third Party Funding

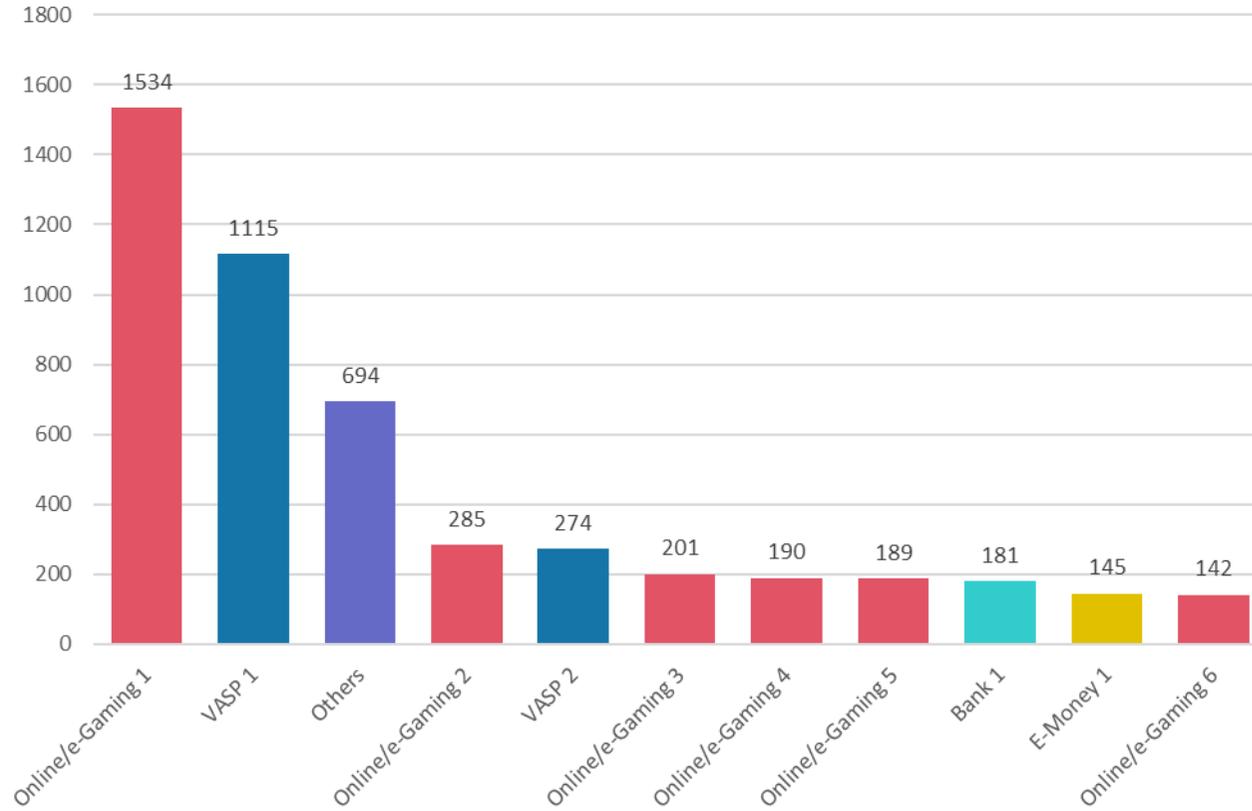


\*Section 1DA/1DAA requests under the Proceeds of Crime are request to relevant financial business for relevant information.



In 2024, the two highest reporting entities were responsible for 54% of all SAR submissions.

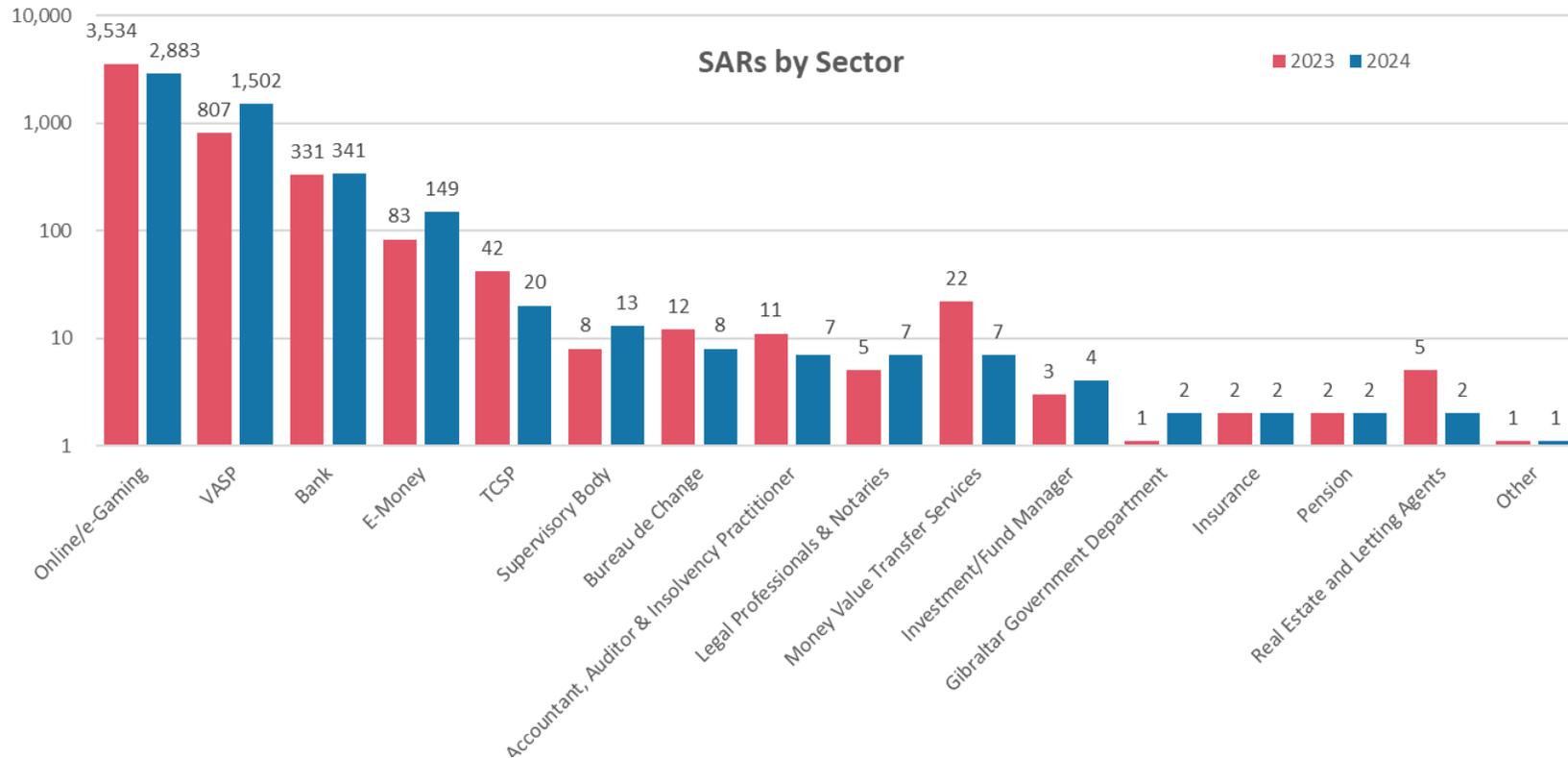
Collectively, the top ten reporting entities accounted for 86% of the total SARs received.



Reporting Sectors

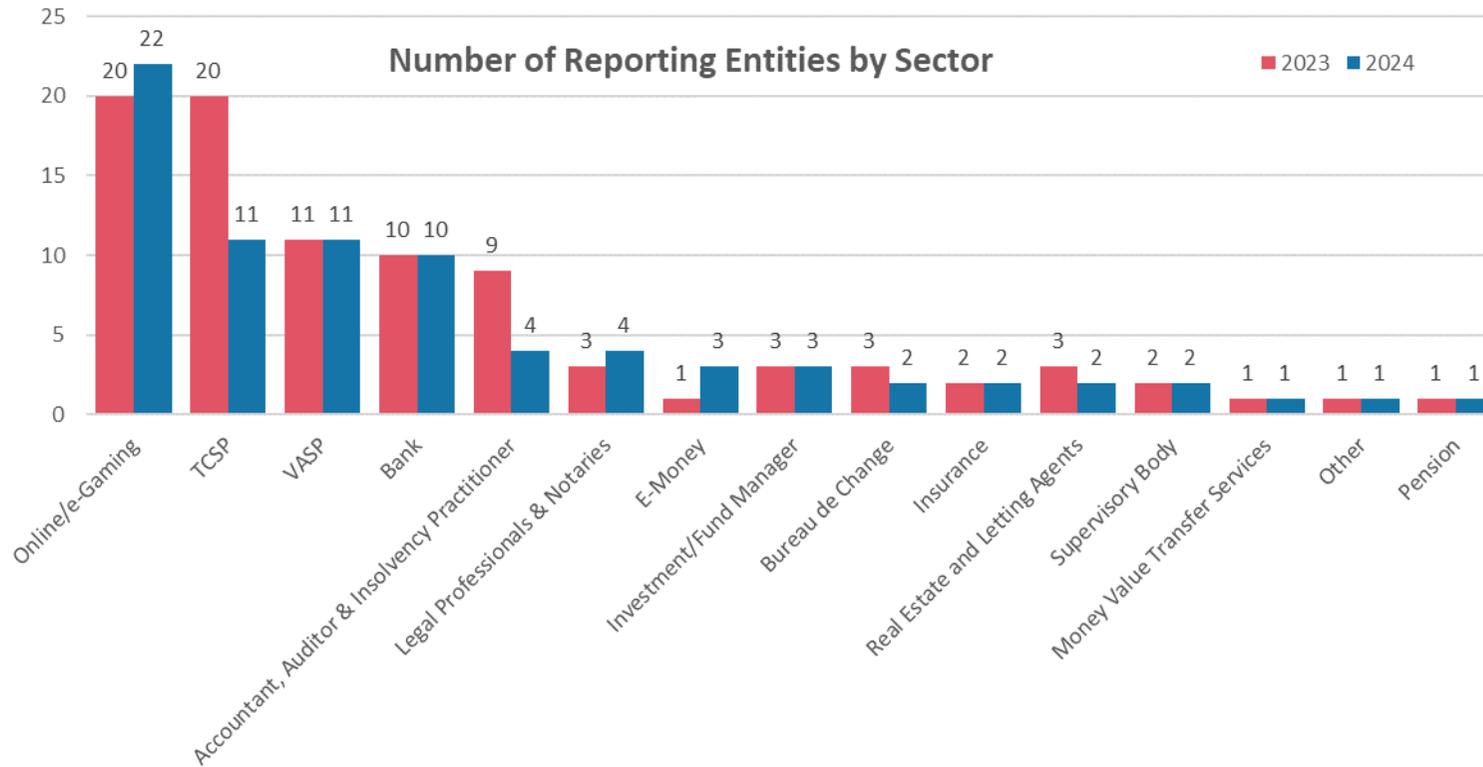
In 2024, a total of 4,950 SARs were received, reflecting a 1.7% increase compared to 2023.

As in previous years, the gaming sector remained the leading source of SARs in 2024, submitting 2,883 reports, accounting for 58% of the total received. However, this marks a significant 18% decline in submissions from the sector. Of these reports, 79% were also dual reported to foreign jurisdictions. In contrast, the VASP sector saw a sharp increase in reporting, accounting for 30% of all SARs. The e-money sector likewise recorded a notable rise in SAR submissions.



In 2024, SARs were submitted by 80 reporting entities across 16 sectors, marking a decrease from 91 reporting entities in 2023. This decline is primarily attributed to a reduction in the number of reporting entities within the TCSP sector.

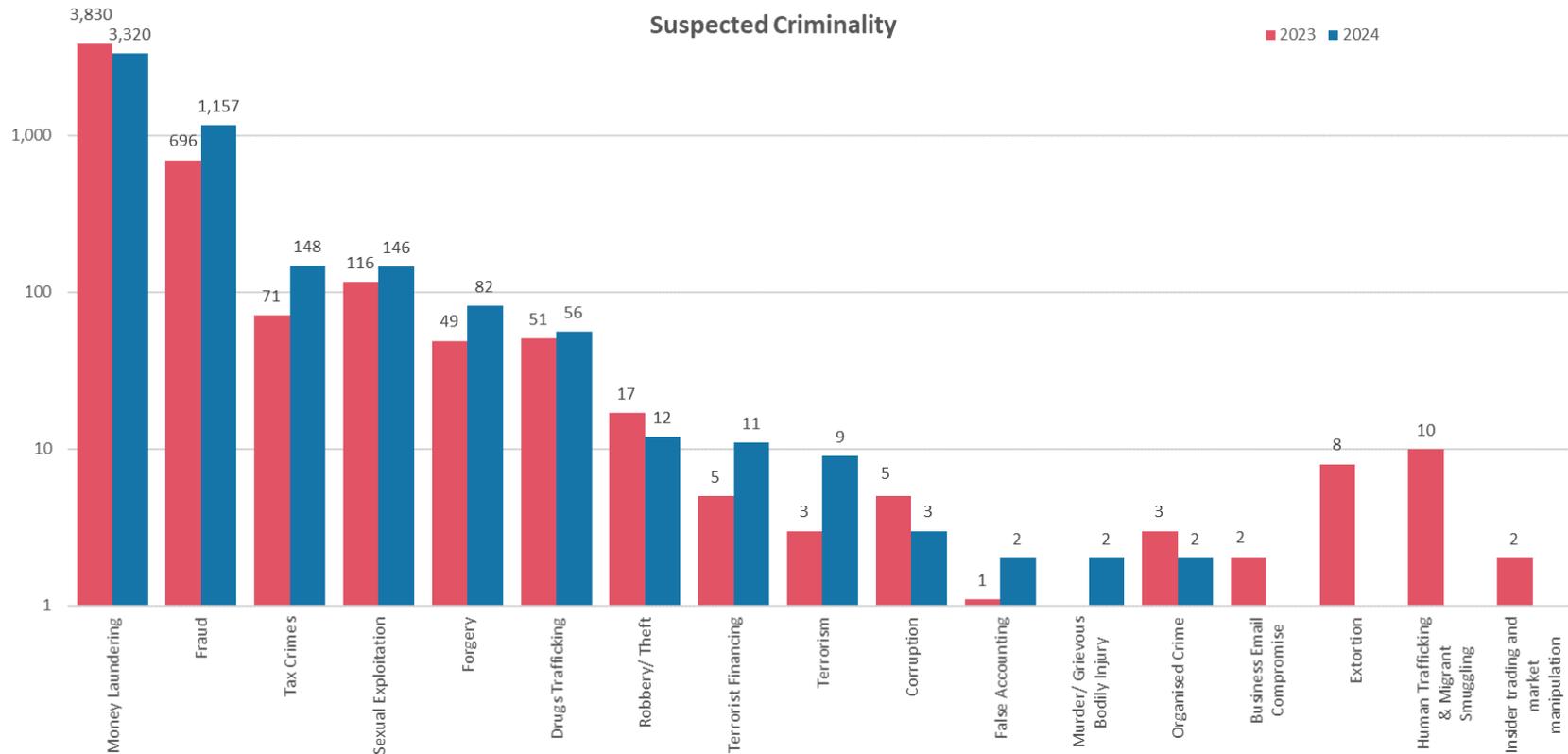
A total of 114 reporting entities submitted SARs over the course of 2023 and 2024.



### Suspected Criminality

As in previous years the suspected criminality selected by the reporter for the SAR did not always correlate with the suspected criminality which gave rise to the suspicion. During the assessment of SARs, the suspected criminality of a number of SARs were changed, primarily to money laundering and fraud.

Money laundering and fraud remain the top reported suspected criminality of SARs. The reporting of fraud experienced a significant increase, primarily from the VASP, online/e-Gaming and banking sectors. A substantial amount of these related to payment fraud, scams and Ponzi schemes.



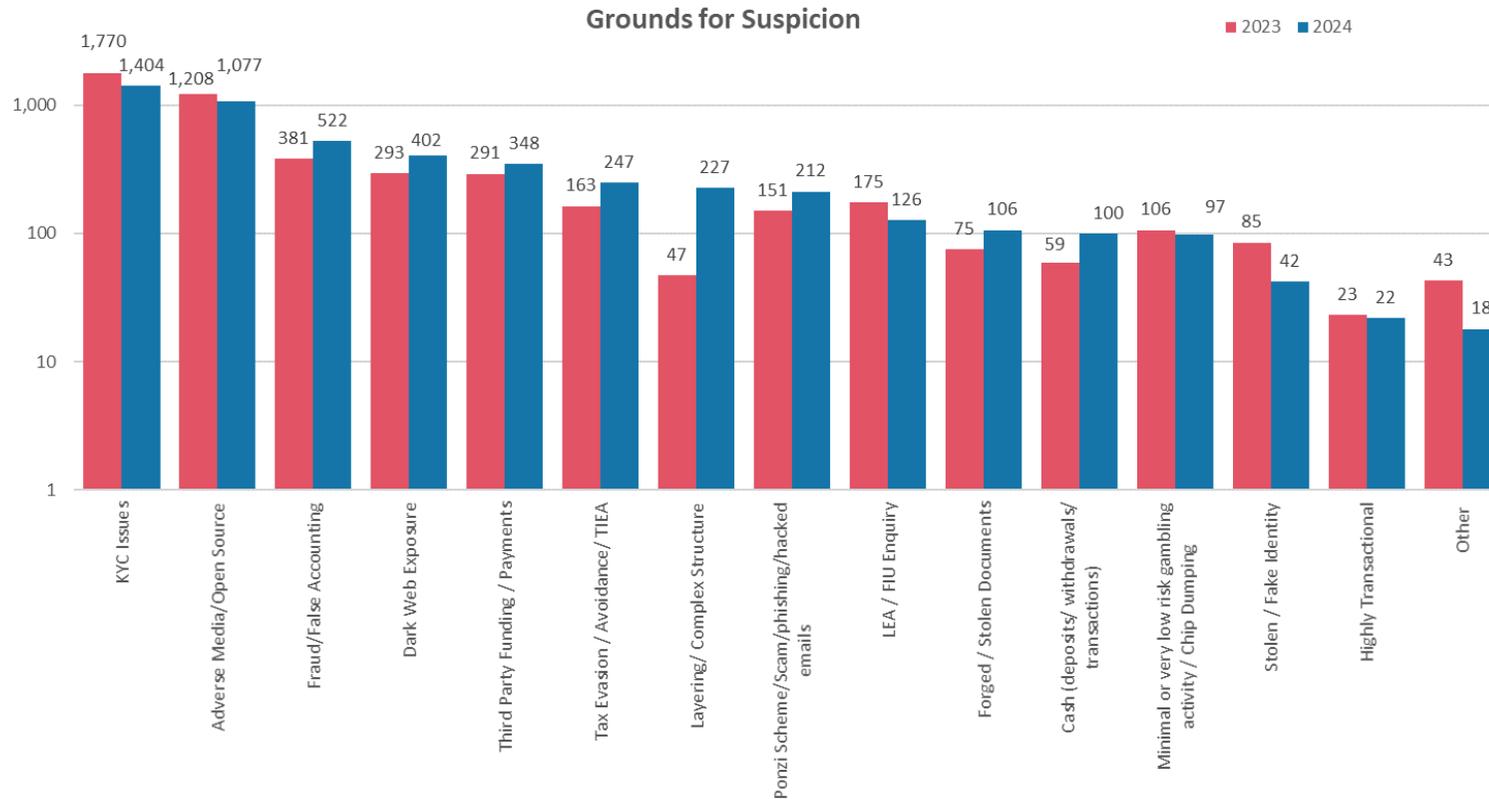
Suspected Criminality	Accountant, Auditor & Insolvency Practitioner	Bank	Bureau de Change	E-Money	Gibraltar Government Department	Insurance	Investment/Fund Manager	Legal Professionals & Notaries	Money Value Transfer Services	Online/e-Gaming	Other	Pension	Real Estate and Letting Agents	Supervisory Body	TCSP	VASP	Total
Corruption	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	1	3
Drugs Trafficking	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	56	56
False Accounting	-	1	-	-	-	-	1	-	-	-	-	-	-	-	-	-	2
Forgery	-	19	-	14	-	-	-	-	-	41	-	-	-	-	-	8	82
Fraud	6	179	1	71	-	1	3	1	-	311	-	1	-	-	3	580	1,157
Money Laundering	1	117	5	55	-	1	-	6	7	2,402	1	-	2	11	11	701	3,320
Murder/ Grievous Bodily Injury	-	-	-	2	-	-	-	-	-	-	-	-	-	-	-	-	2
Organised Crime	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	1	2
Robbery/ Theft	-	-	-	-	-	-	-	-	-	8	-	-	-	-	-	4	12
Sexual Exploitation	-	2	1	1	-	-	-	-	-	-	-	-	-	-	1	141	146
Tax Crimes	-	19	1	3	2	-	-	-	-	113	-	1	-	1	3	5	148
Terrorism	-	-	-	2	-	-	-	-	-	4	-	-	-	-	1	2	9
Terrorist Financing	-	2	-	1	-	-	-	-	-	4	-	-	-	-	1	3	11
<b>Total</b>	<b>7</b>	<b>341</b>	<b>8</b>	<b>149</b>	<b>2</b>	<b>2</b>	<b>4</b>	<b>7</b>	<b>7</b>	<b>2,883</b>	<b>1</b>	<b>2</b>	<b>2</b>	<b>13</b>	<b>20</b>	<b>1,502</b>	<b>4,950</b>



## Grounds for Suspicion

In 2024, the largest proportion of SARs, accounting for 28%, were submitted due to Know Your Customer (KYC) related issues, primarily concerning the failure to provide adequate KYC information and source of funds documentation. Additionally, 22% of SARs were submitted based on adverse media and open source intelligence findings.

The VASP sector observed a surge in reports related to layering, particularly in the use of Bitcoin ATM, conversion to fiat currencies and then transferred to bank accounts.



Grounds for Suspicion	Adverse Media/Open Source	Cash (deposits/ withdrawals/ transactions)	Dark Web Exposure	Forged / Stolen Documents	Fraud/False Accounting	Minimal or very low risk gambling activity / Chip Dumping	High Risk Country	Highly Transactional	KYC Issues	Layering/ Complex Structure	LEA / FIU Enquiry	Ponzi Scheme/Scam/phishing/ hacked emails	Sanctions (Gibraltar / UK / UN / EU)	Stolen / Fake Identity	Tax Evasion / Avoidance/ TIEA	Third Party Funding / Payments	Use of deceased person's account	Other	Total	
Accountant, Auditor & Insolvency Prac	1	-	-	-	4	-	-	-	-	1	-	1	-	-	-	-	-	-	-	7
Bank	17	15	-	25	107	-	2	4	32	23	12	37	-	15	20	31	1	-	-	341
Bureau de Change	3	1	-	-	1	-	-	-	2	-	-	-	-	-	1	-	-	-	-	8
E-Money	4	10	-	15	61	-	-	3	15	21	6	5	-	1	3	5	-	-	-	149
Gibraltar Government Department	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	2
Insurance	1	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2
Investment/Fund Manager	1	-	-	-	2	-	-	-	1	-	-	-	-	-	-	-	-	-	-	4
Legal Professionals & Notaries	-	1	-	1	-	-	-	-	2	1	1	-	-	-	-	-	-	-	1	7
Money Value Transfer Services	-	1	-	-	-	-	-	1	-	2	-	-	-	-	-	3	-	-	-	7
Online/e-Gaming	1,005	66	-	55	67	97	7	3	938	58	93	1	-	18	208	264	3	-	-	2,883
Other	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1
Pension	-	-	-	-	1	-	-	-	-	-	-	-	-	-	1	-	-	-	-	2
Real Estate and Letting Agents	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2
Supervisory Body	2	1	-	-	-	-	-	-	7	-	-	-	-	-	1	-	-	-	2	13
TCSP	3	-	-	1	1	-	-	-	9	1	-	1	-	-	3	-	-	-	1	20
VASP	38	4	402	9	277	-	-	11	398	120	14	167	1	8	8	45	-	-	-	1,502
<b>Total</b>	<b>1,077</b>	<b>100</b>	<b>402</b>	<b>106</b>	<b>522</b>	<b>97</b>	<b>9</b>	<b>22</b>	<b>1,404</b>	<b>227</b>	<b>126</b>	<b>212</b>	<b>1</b>	<b>42</b>	<b>247</b>	<b>348</b>	<b>4</b>	<b>4</b>	<b>4,950</b>	



## SARs with a Gibraltar nexus

As an International Finance Centre, Gibraltar attracts a high volume of SARs, most of which relate to activity with international dimensions. This reflects the global reach of its financial sector and the compliance of its reporting entities. In 2024, 134 SARs were identified as having a Gibraltar nexus, equivalent to 2.7% of all SARs received, demonstrating that while domestic links are limited, local institutions remain alert to potential threats. The banking sector led domestic reporting, accounting for 54% of these Gibraltar-linked SARs. Although fewer SARs translate into domestic investigations, this highlights Gibraltar's strong international cooperation and the GFIU's strategic focus on targeting criminality beyond its borders, reinforcing the jurisdiction's standing as a trusted and effective contributor to global AML/CFT/CPF efforts.

Sector	False Accounting	Forgery	Fraud	Money Laundering	Organised Crime	Sexual Exploitation	Tax Crimes	Terrorism	Terrorist Financing	Total
Accountant, Auditor & Insolvency Practitioner	-	-	4	1	-	-	-	-	-	5
Bank	-	-	32	29	-	-	12	-	-	73
Bureau de Change	-	-	1	5	-	1	1	-	-	8
E-Money	-	1	2	1	-	-	-	1	-	5
Gibraltar Government Department	-	-	-	-	-	-	2	-	-	2
Insurance	-	-	-	1	-	-	-	-	-	1
Investment/Fund Manager	1	-	-	-	-	-	-	-	-	1
Legal Professionals & Notaries	-	-	-	4	-	-	-	-	-	4
Money Value Transfer Services	-	-	-	7	-	-	-	-	-	7
Online/e-Gaming	-	-	1	2	-	-	-	-	-	3
Other	-	-	-	1	-	-	-	-	-	1
Pension	-	-	1	-	-	-	-	-	-	1
Real Estate and Letting Agents	-	-	-	1	-	-	-	-	-	1
Supervisory Body	-	-	-	9	1	-	1	-	-	11
TCSP	-	-	1	7	-	-	1	-	1	10
VASP	-	-	-	1	-	-	-	-	-	1
<b>Total</b>	<b>1</b>	<b>1</b>	<b>42</b>	<b>69</b>	<b>1</b>	<b>1</b>	<b>17</b>	<b>1</b>	<b>1</b>	<b>134</b>



## Defensive SARs

Defensive SARs refer to a well-known practice whereby entities adopt overly inclusive detection criteria to mitigate perceived regulatory or reputational risk. Such reports are typically identified when, upon the operational analysis stage by the GFIU, the activity or transaction in question is assessed as not deemed suspicious or having been triggered by suspicion raised by the reporting entity.

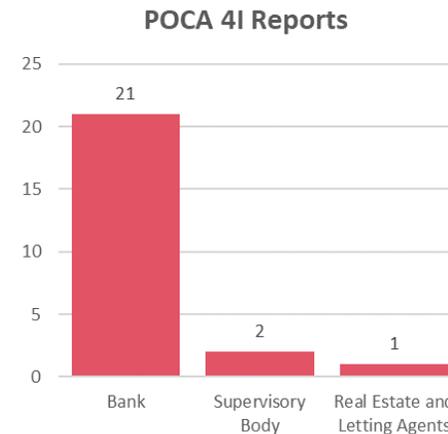
These types of submissions can compromise the overall effectiveness of the SAR regime by generating disclosures that erroneously categorise legitimate behaviour as suspicious, thereby diluting the value of intelligence.

In response, the GFIU's targeted outreach programme, Project Nexus, has contributed to a substantial reduction in the volume of defensive SARs. As of 2024, only 0.7% of SARs were classified as defensive by the GFIU's analysis, a significant decline from 25% recorded in 2019. This shift strengthens the integrity and intended function of the SAR regime by promoting more targeted, risk focused, and actionable intelligence.

## 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 2024, a total of 24 reports were submitted under Section 4I of POCA, originating from three different reporting sectors.

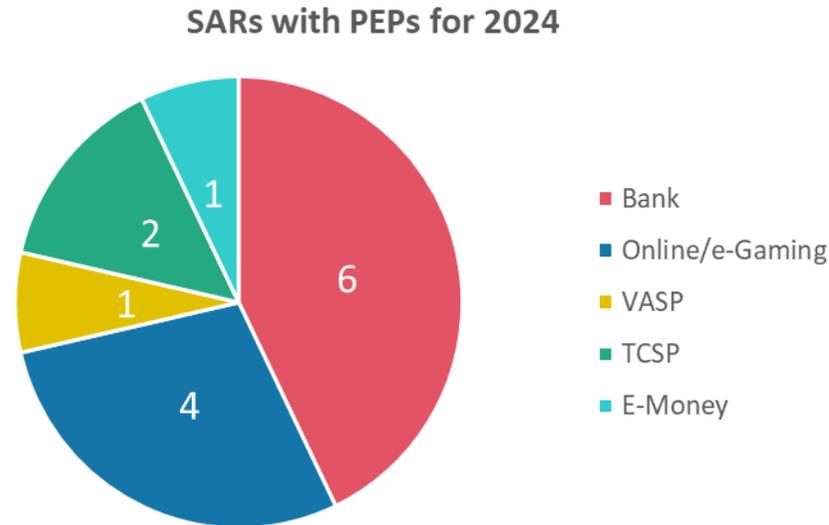


## Politically Exposed Persons

When submitting a SAR, MLROs are required to report any links to, or identification of, Politically Exposed Persons (PEPs). A recent 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 2024, 14 SARs were submitted identifying a PEP as a subject.

The chart below shows the numbers of PEP connected SARs per sector submitted during 2024.



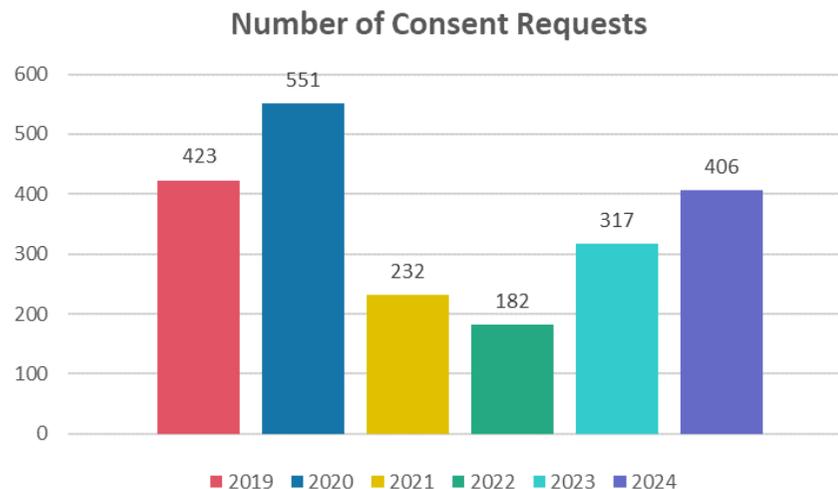
## Consent Requests

In 2024, the GFIU received a total of 406 consent requests, including those linked to SARs submitted in previous years. This represents a 28% increase compared to 2023, continuing the upward trend observed that year.

While consent is the formal legal term used under the relevant legislative framework, the GFIU refers to these as “Defence Against Money Laundering” (DAML) requests to promote clearer understanding among stakeholders. Consent requests are submitted by reporting entities when seeking approval from the GFIU before proceeding with a transaction suspected to involve criminal property, allowing the GFIU to assess whether further action is warranted.

Consent requests were submitted across nine reporting sectors in 2024, with the highest volumes originating from the gaming sector (167 requests) and the banking sector (140 requests). The GFIU maintained an average response time of four working days, ensuring prompt handling of these time sensitive matters.

Of the 341 SARs submitted by the banking sector in 2024, 88 included consent requests, approximately 25% of the sector’s total submissions. Several of these SARs involved multiple consent requests, reflecting the sector’s active role in identifying suspected criminal property



A total of 46 consent 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.

Additionally, two consent requests were submitted in error and did not require a formal response.

Sector	Consent						Total
	Consent Granted	Consent Not Applicable	Consent Refused	Consent Rescinded	Consent Subsequently Granted	No Response Required	
Accountant, Auditor & Insolvency Practitioner	1	1	-	-	-	-	2
Bank	123	15	-	1	1	-	140
E-Money	6	-	-	-	-	-	6
Insurance	1	-	-	-	-	-	1
Legal Professionals & Notaries	1	-	-	-	-	-	1
Online/e-Gaming	149	16	-	-	-	2	167
Pension	-	1	-	-	-	-	1
TCSP's	2	2	-	-	-	-	4
VASP	71	11	1	-	1	-	84
<b>Total</b>	<b>354</b>	<b>46</b>	<b>1</b>	<b>1</b>	<b>2</b>	<b>2</b>	<b>406</b>



More than half of the consent requests received were linked to SARs involving suspected money laundering, while approximately a fifth were associated with suspected fraud.

Suspected Criminality	Consent						Total
	Consent Granted	Consent Not Applicable	Consent Refused	Consent Rescinded	Consent Subsequently Granted	No Response Required	
Corruption	5	-	-	-	-	-	5
Forgery	8	-	-	-	-	-	8
Fraud	82	10	-	-	-	-	92
Insider trading and market manipulation	6	-	-	-	-	-	6
Miscellaneous	2	3	1	-	1	-	7
Money Laundering	226	23	-	1	1	2	253
Sexual Exploitation	-	2	-	-	-	-	2
Tax Crimes	25	6	-	-	-	-	31
Terrorist Financing	-	2	-	-	-	-	2
<b>Total</b>	<b>354</b>	<b>46</b>	<b>1</b>	<b>1</b>	<b>2</b>	<b>2</b>	<b>406</b>



In 2024, a total of 308 SARs included consent requests, with 33 of these involving multiple requests. The banking sector was the primary submitter of SARs with multiple consent requests, including one SAR that generated eight separate requests.

The table below shows the number of consent request received in 2024 per sector and number of consent requests per SAR.

Sector	Number of consent requests per SAR					Total
	1	2	3	6	8	
Accountant, Auditor & Insolvency Practitioner	2	-	-	-	-	2
Bank	72	18	6	1	1	98
E-Money	6	-	-	-	-	6
Insurance	1	-	-	-	-	1
Legal Professionals & Notaries	1	-	-	-	-	1
Online/e-Gaming	147	10	-	-	-	157
Pension	1	-	-	-	-	1
TCSP's	2	1	-	-	-	3
VASP	76	4	-	-	-	80
<b>Total</b>	<b>308</b>	<b>33</b>	<b>6</b>	<b>1</b>	<b>1</b>	<b>349</b>



Consent requests received in 2024 were linked to activities across 61 jurisdictions where the grounds for suspicion arose. Of the consent requests having a Gibraltar nexus, three quarters originated from the banking sector.

The table below shows the top ten jurisdictions.

Jurisdiction	Accountant, Auditor & Insolvency Practitioner	Bank	DLT Provider	E-Money	Insurance	Legal Professionals & Notaries	Online/e-Gaming	Pension	TCSP's	Total
United Kingdom	1	27	12	5	-	-	29	-	-	74
Brazil	-	1	5	-	-	-	54	-	-	60
Ireland	-	-	1	-	-	-	28	-	-	29
Gibraltar	1	21	1	-	1	-	-	1	3	28
Canada	-	-	-	-	-	-	23	-	-	23
Mexico	-	3	18	-	-	-	1	-	-	22
Argentina	-	6	8	-	-	-	-	-	-	14
China	-	14	-	-	-	-	-	-	-	14
Switzerland	-	7	1	-	-	-	3	-	-	11
Bolivia	-	-	11	-	-	-	-	-	-	11



### Findings of the Feedback Provided to the Reporter

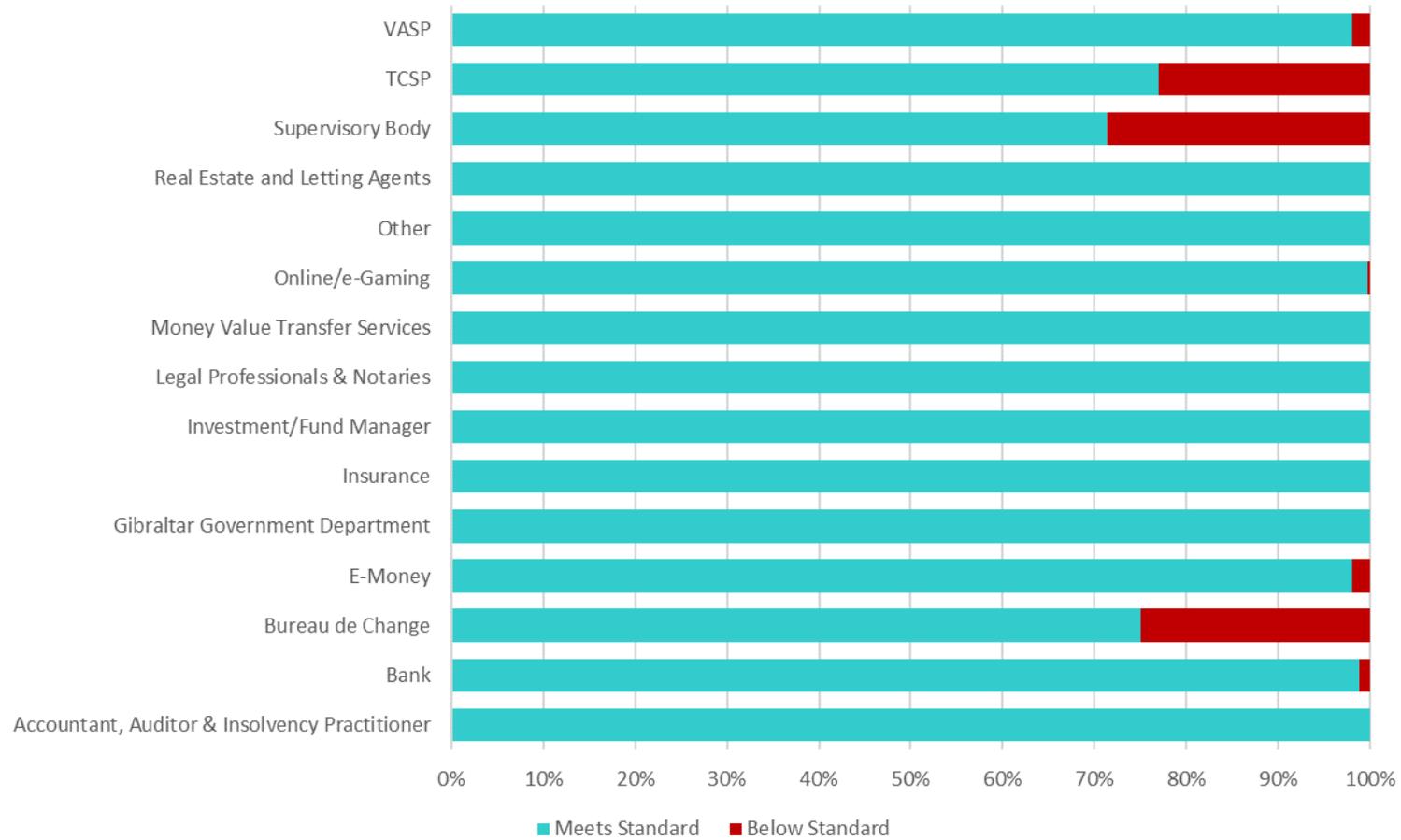
The GFIU continues to assess the quality of SARs submitted by Reporting Entities, including Money Laundering Reporting Officers and Nominated Officers. Structured feedback is issued as part of the GFIU's ongoing efforts to promote the submission of high-quality intelligence and to support compliance with legal and regulatory obligations.

SARs are evaluated against five core criteria, with each submission assigned a quality rating based on the following elements:

1. The SAR must be accompanied by all relevant supporting material necessary to enable effective operational and strategic analysis by the GFIU.
2. The report must clearly articulate a suspicion of a predicate offence, money laundering, or terrorist financing, based on the information disclosed.
3. Sufficient detail must be provided regarding the reporting entity's relationship with the subject(s) of the SAR, including the nature and context of the interaction.
4. The SAR's narrative must be well-structured, coherent, and comprehensive, ensuring that all relevant facts are presented clearly to facilitate timely analysis.
5. Where a Defence Against Money Laundering (DAML) request is made, the SAR must explicitly identify the suspicion (within the grounds for suspicion), the suspected criminal property, and the prohibited act in accordance with the Proceeds of Crime Act 2015.

Analysis of SARs submitted in 2024 indicates that 98% met or exceeded the quality threshold, reflecting the positive impact of the GFIU's outreach and engagement initiatives. For SARs assessed as falling below the required standard, tailored feedback was provided to the relevant Reporting Entity. This included a breakdown of deficiencies and constructive recommendations aimed at improving future submissions. Where necessary, follow-up support was offered through Project Nexus engagement clinics or through referral to the relevant e-learning workshops hosted on the GFIU's e-Nexus platform.

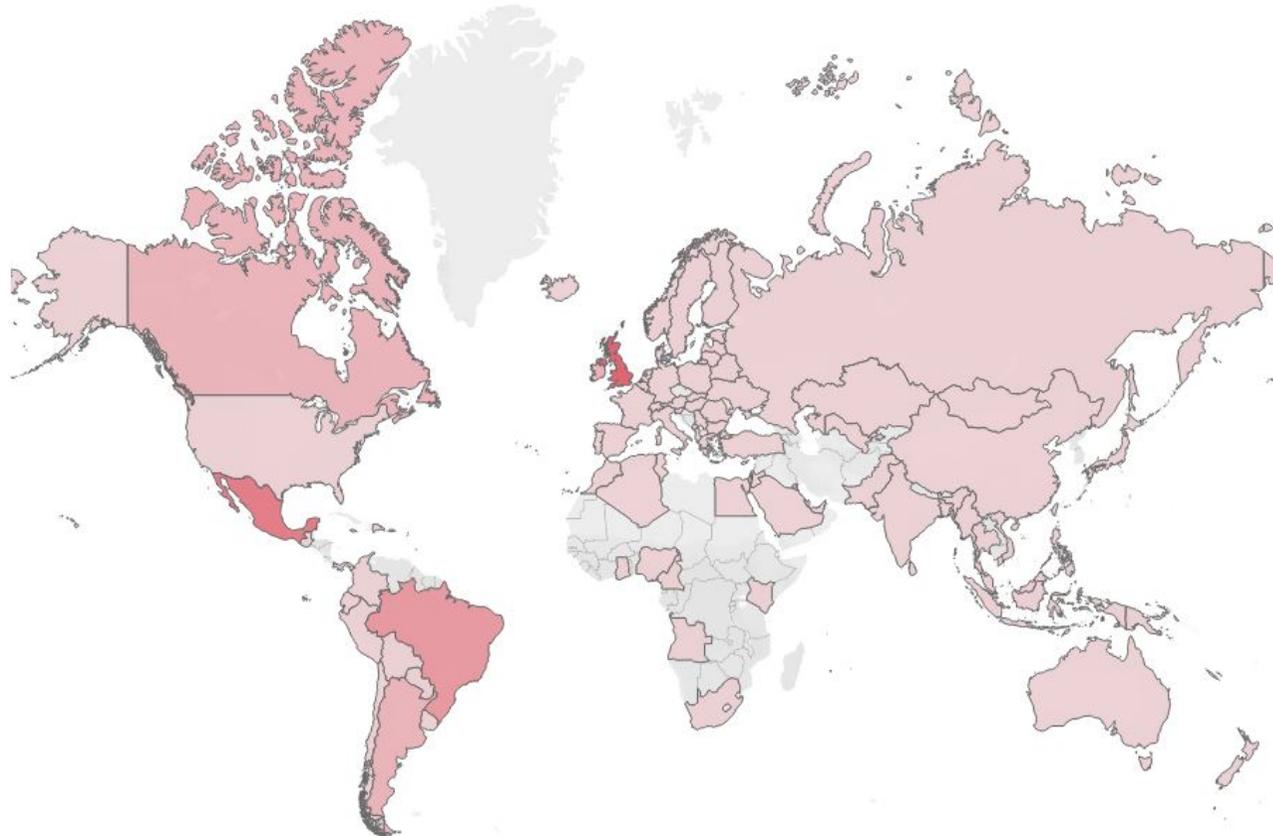




## SARs Reported by Jurisdiction

In 2024, SARs received were linked to 100 jurisdictions. As seen in previous years, the majority of SARs (53%) had a UK nexus. The gaming sector reported most of these, with suspected criminal activities primarily involving money laundering or fraud. There was a significant increase in SARs with a Mexican nexus, nearly all of which were reported by the VASP sector, with money laundering and fraud being the predominant suspected criminal activities.

The chart below shows a heat map of the SARs received in 2024 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 deemed to have occurred.

Jurisdiction	Corruption	Drugs Trafficking	False Accounting	Forgery	Fraud	Money Laundering	Murder/ Grievous Bodily Injury	Organised Crime	Robbery/ Theft	Sexual Exploitation	Tax Crimes	Terrorism	Terrorist Financing	Total
United Kingdom	1	31	1	52	522	1,942	1	-	6	5	59	4	6	2630
Mexico	-	1	-	2	341	413	-	-	4	105	1	1	1	869
Brazil	-	-	-	4	23	257	-	-	-	20	40	-	-	344
Gibraltar	-	-	1	1	42	69	-	1	-	1	17	1	1	134
Ireland	-	-	-	-	5	126	-	-	1	-	-	1	1	134
Argentina	-	-	-	1	25	96	-	-	-	8	-	1	1	132
Canada	-	-	-	-	6	104	-	-	-	-	10	1	-	121
Kuwait	-	-	-	1	-	93	-	-	1	-	-	-	-	95
Bolivia	-	-	-	-	29	3	-	-	-	-	-	-	-	32
Spain	-	3	-	-	12	10	-	-	-	-	4	-	-	29
<b>Total</b>	<b>1</b>	<b>35</b>	<b>2</b>	<b>61</b>	<b>1005</b>	<b>3113</b>	<b>1</b>	<b>1</b>	<b>12</b>	<b>139</b>	<b>131</b>	<b>9</b>	<b>10</b>	<b>4520</b>



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

Jurisdiction	Corruption	Drugs Trafficking	False Accounting	Forgery	Fraud	Money Laundering	Murder/ Grievous Bodily Injury	Organised Crime	Robbery/ Theft	Sexual Exploitation	Tax Crimes	Terrorism	Terrorist Financing	Total
Mexico	-	1	-	2	341	412	-	-	4	105	1	1	1	868
United Kingdom	1	31	1	19	222	128	1	-	-	5	6	2	3	419
Gibraltar	-	-	1	1	41	67	-	1	-	1	17	1	1	131
Argentina	-	-	-	1	25	94	-	-	-	8	-	1	1	130
Brazil	-	-	-	2	21	77	-	-	-	20	-	-	-	120
Bolivia	-	-	-	-	29	1	-	-	-	-	-	-	-	30
Spain	-	3	-	-	12	10	-	-	-	-	4	-	-	29
China	-	-	-	2	15	6	-	-	-	-	1	-	-	24
Colombia	-	-	-	-	8	14	-	-	-	-	-	-	-	22
Australia	-	2	-	2	14	2	-	-	-	1	-	-	-	21
<b>Total</b>	<b>1</b>	<b>37</b>	<b>2</b>	<b>29</b>	<b>728</b>	<b>811</b>	<b>1</b>	<b>1</b>	<b>4</b>	<b>140</b>	<b>29</b>	<b>5</b>	<b>6</b>	<b>1794</b>



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	1	87	-	142	-	1	2	-	-	2,211	-	-	-	-	2	184	<b>2,630</b>
Mexico	-	2	-	-	-	-	-	-	-	1	-	-	-	-	-	866	<b>869</b>
Brazil	-	2	-	-	-	-	-	-	-	224	-	-	-	-	-	118	<b>344</b>
Gibraltar	5	73	8	5	2	1	1	4	7	3	1	1	1	11	10	1	<b>134</b>
Ireland	-	1	-	1	-	-	-	-	-	125	-	-	-	-	-	7	<b>134</b>
Argentina	-	9	-	-	-	-	-	-	-	2	-	-	-	-	-	121	<b>132</b>
Canada	-	3	-	-	-	-	-	-	-	117	-	-	-	-	-	1	<b>121</b>
Kuwait	-	-	-	-	-	-	-	-	-	95	-	-	-	-	-	-	<b>95</b>
Bolivia	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-	30	<b>32</b>
Spain	-	12	-	-	-	-	-	1	-	-	-	-	1	-	1	14	<b>29</b>
<b>Total</b>	<b>6</b>	<b>189</b>	<b>8</b>	<b>148</b>	<b>2</b>	<b>2</b>	<b>3</b>	<b>5</b>	<b>7</b>	<b>2,780</b>	<b>1</b>	<b>1</b>	<b>2</b>	<b>11</b>	<b>13</b>	<b>1,342</b>	<b>4,520</b>



## 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 21 February 2025. Other jurisdictions are on the lists but are not mentioned in reports received by the GFU, therefore they have been excluded from the report.

<b>FATF high risk and increased monitoring rated jurisdictions</b>	<b>No. of SARs</b>
Algeria	5
Angola	8
Bulgaria	9
Cameroon	4
Kenya	1
Monaco	1
Nigeria	11
South Africa	8
Viet Nam	4
<b>No. of SARs with a link to a FATF high risk and increased monitoring rated jurisdictions</b>	<b>51</b>
<b>Total number of SARs</b>	<b>4950</b>
<b>% of SARs reported with link to a FATF high risk and increased monitoring rated jurisdictions</b>	<b>1.03%</b>



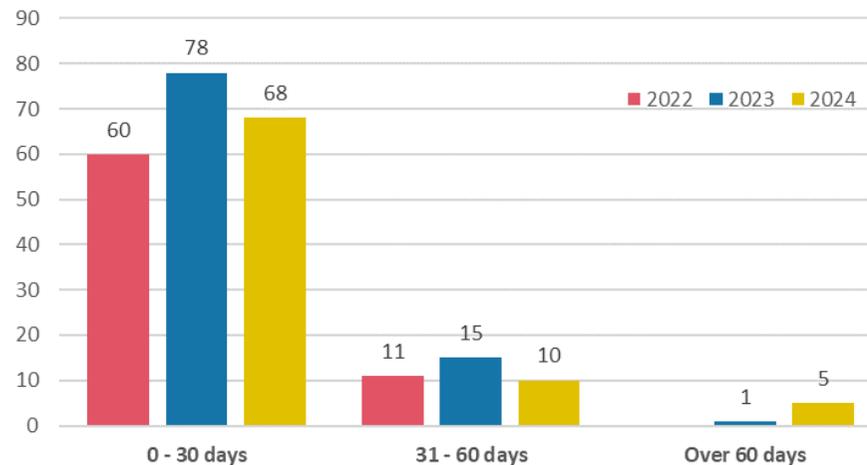
## Egmont Requests and Spontaneous Intelligence

Egmont requests are requests from foreign FIUs for intelligence held by the GFIU, external databases and third parties. These exchanges of information are conducted via the Egmont Secure Web. All requests are recorded in Themis, which allows linking of subjects either contained in GFIU data or Mutual Legal Assistance requests.

The Egmont Group of Financial Intelligence Units has outlined suggested response times for requests received by FIUs, emphasising the importance of timely replies, whether affirmative or negative. While acknowledging that response times may vary depending on the nature of the requests, Egmont typically recommends that responses be provided within one month, if feasible. It's recognised that additional time may be necessary when querying external databases or involving third parties.

Despite the need to consult external databases or third parties for every Egmont request received by the GFIU, a notable 82% were successfully addressed within the recommended 30 day period. Factors that can affect response times include the GFIU's detailed analysis of requests, potential follow-up actions, consultations with law enforcement agencies or other authorities, and instances where clarification from the requesting FIU is needed. These factors, along with risk assessments related to information sharing, reflect the complexity and diligence required in handling foreign intelligence requests efficiently.

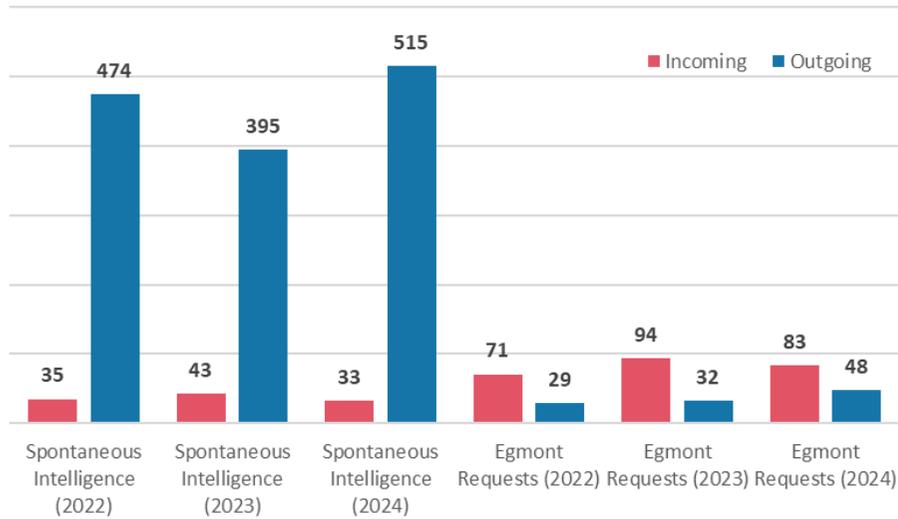
The chart below shows the timeframe for the GFIU to respond to Egmont Requests.



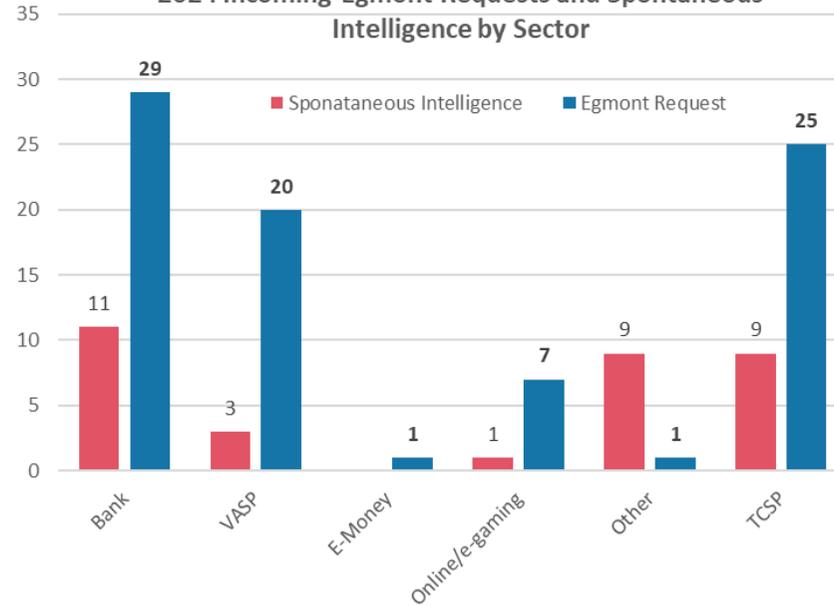
In 2024, the number of incoming Egmont requests decreased by 12% compared to 2023. Most of these requests relate to the banking, TCSP and VASP sectors. Conversely, outgoing Egmont requests experienced a significant rise, increasing by 50% from the previous year.

Additionally, the volume of outgoing spontaneous intelligence reports grew by 30% in 2024 compared to 2023.

### Egmont Requests and Spontaneous Intelligence 2022-2024



### 2024 Incoming Egmont Requests and Spontaneous Intelligence by Sector



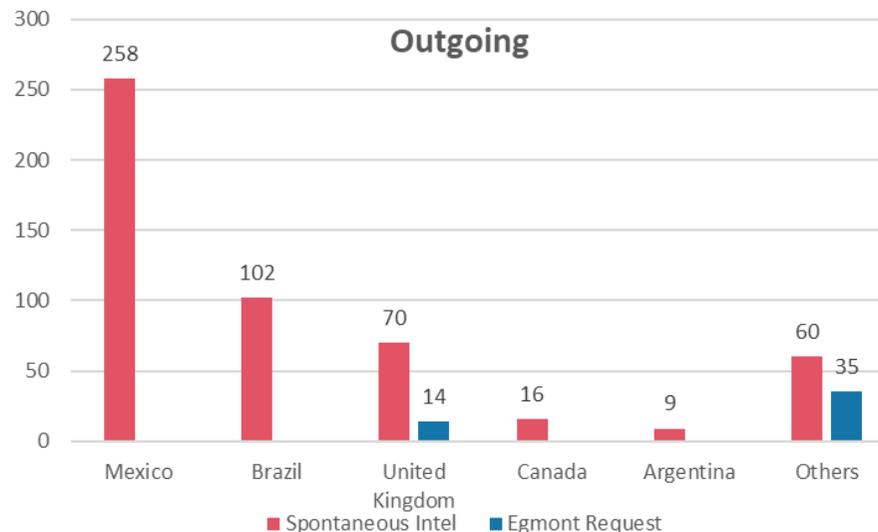
In 2024, the GFIU continued to actively engage in international cooperation through both formal and spontaneous channels. A total of 83 requests were received from 28 foreign jurisdictions via the Egmont Secure Web (ESW), while 48 outgoing requests were issued to 24 jurisdictions, reflecting a balanced and responsive approach to international intelligence-sharing.

In addition to formal requests, the GFIU received 33 spontaneous intelligence reports from 15 jurisdictions and disseminated 515 spontaneous intelligence reports to 36 jurisdictions. These disseminations were based on SARs received in both 2024 and previous reporting periods. While certain SARs received in 2024 have also led to disseminations in 2025, these are excluded from the statistics presented in this report to maintain temporal consistency in the data.

The United Kingdom remained the principal counterpart for Egmont exchanges, accounting for 21 incoming and 14 outgoing requests, underscoring its central role in cross-border financial intelligence collaboration. In terms of spontaneous intelligence, Mexico and Brazil were the most frequent recipients, mirroring their consistent appearance among the top jurisdictions cited in SARs.

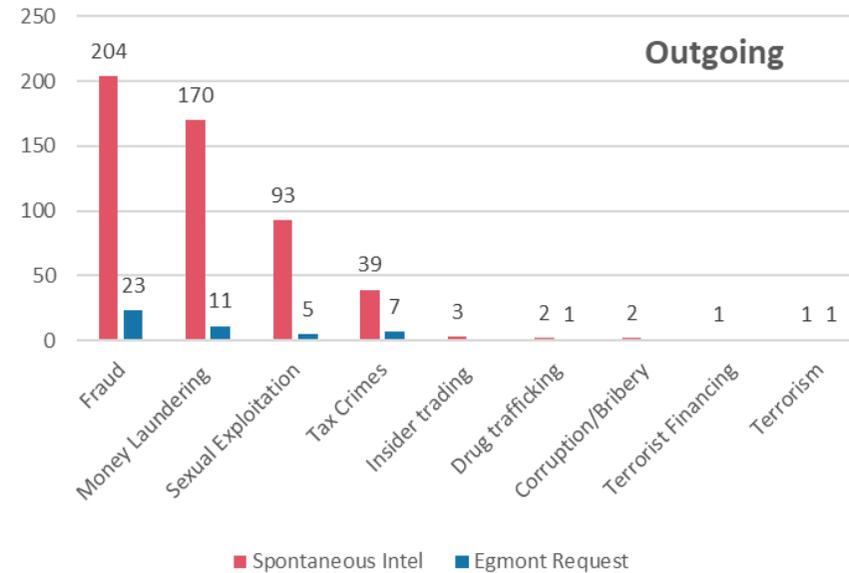
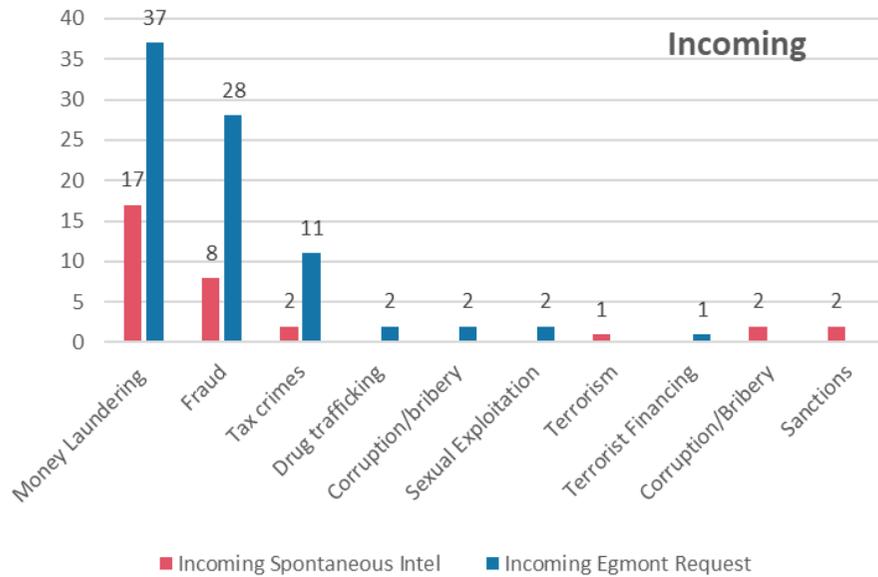
Although the United Kingdom continues to be the most frequently referenced jurisdiction in SARs, it is important to note that a substantial portion of these are dual reported directly to UK authorities.

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 in 2024, suspected sexual exploitation ranked third among the criminal activities linked to outgoing spontaneous intelligence. These cases originate from SARs submitted by the VASP sector, highlighting suspected direct or indirect involvement in the distribution and receipt of child abuse material via the darknet.

The tables below show the top suspected criminality for incoming and outgoing Egmont requests and spontaneous intelligence for 2024.



## Intelligence Reports Disseminated to Local Law Enforcement Agencies & Supervisory Bodies

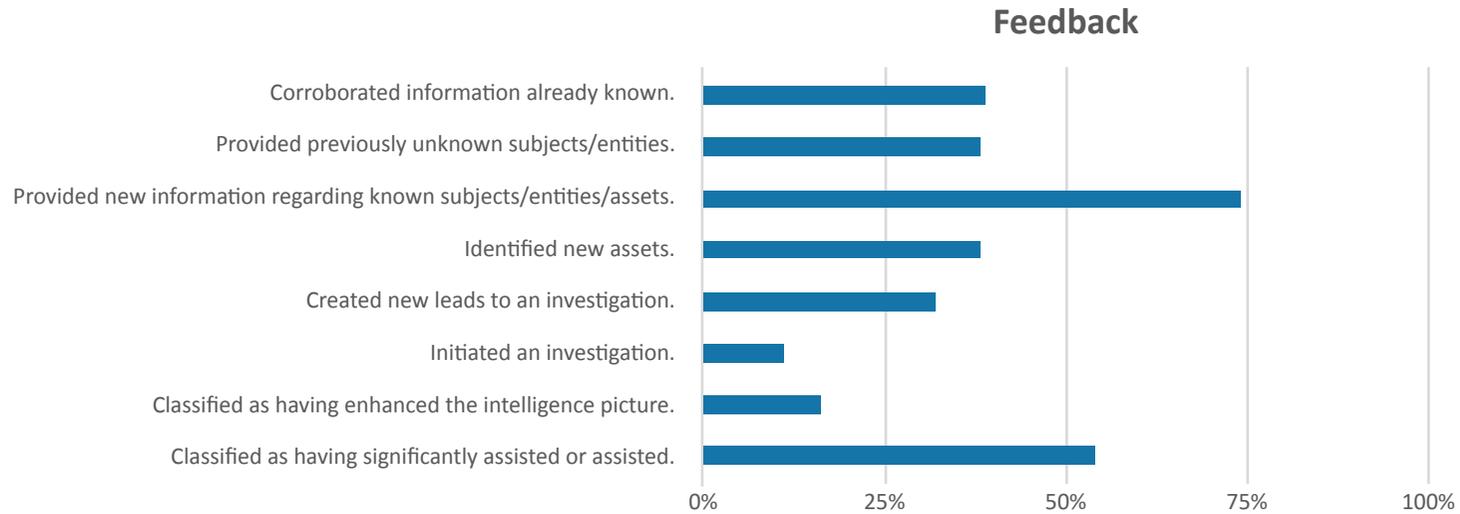
The GFIU disseminates Intelligence Reports to Law Enforcement Agencies and Supervisory Bodies when considered relevant. These reports are produced based on a range of intelligence sources received by the GFIU.

The following Intelligence Reports were disseminated during 2024.

LEA/Authority	Corruption/Bribery	Drug trafficking	Forgery	Fraud	Money Laundering	Organised crime	Robbery/theft	Sanctions	Smuggling	Tax crimes	Terrorism	Terrorist Financing	Total
Gaming Division	-	-	-	2	-	-	-	-	-	-	-	-	2
Gibraltar Financial Services Commission	-	-	-	4	3	1	-	2	-	-	-	-	10
HM Customs	-	2	1	-	7	-	-	-	6	3	-	-	19
Joint Financial Intelligence Tasking Group	-	-	-	2	6	-	-	1	-	-	-	-	9
Legal Services Regulatory Authority	-	-	-	-	1	-	-	-	-	-	-	-	1
Office of Fair Trading	-	-	-	1	2	-	-	-	-	1	-	-	4
RGP (Economic Crime Unit)	1	6	-	31	21	-	1	2	-	4	2	-	68
RGP (Special Branch)	-	-	-	-	3	-	-	-	-	-	6	5	14
Sanctions Competent Authority	-	-	-	-	-	-	-	6	-	-	-	-	6
Tax Authority	-	-	-	1	2	-	-	-	-	6	-	-	9
<b>Total</b>	<b>1</b>	<b>8</b>	<b>1</b>	<b>41</b>	<b>45</b>	<b>1</b>	<b>1</b>	<b>11</b>	<b>6</b>	<b>14</b>	<b>8</b>	<b>5</b>	<b>142</b>



During 2024, feedback was received from Law Enforcement Agencies and Supervisory Bodies regarding the use and impact of Intelligence Reports disseminated both in 2024 and in preceding years. The feedback provided insight into how these reports contributed to operational and strategic outcomes, with the following key highlights identified:





**TCSP**

The owners of an overseas-based business were approached by a company offering to acquire it through a share purchase. The initial contact was made by an individual identifying as a finance executive. A follow-up meeting was held outside the jurisdiction of the business at the acquiring party's request.

During the meeting, the business owners were informed that the intended buyer was a private individual. A substantial monetary offer was made, along with an agreement that the current owners would remain in operational roles for a period of two years. A commission payment, (significant in value) was requested via cryptocurrency transfer.

The owners sought professional advice. Upon review, the service provider identified red flags, including similarities with a previous attempted fraud case involving a similar business. Additional due diligence requests went unanswered, raising further suspicion of fraudulent intent.



**Bank**

A subject opened a prepaid account early in the year, and over a five-month period, approximately £90,000 was deposited through numerous card transactions initiated by third parties; almost the entire amount was withdrawn exclusively in cash via ATMs, with no recorded purchases or other transaction types, behaviour that presents a red flag, as it is consistent with the layering and integration stages of money laundering and indicative of attempts to obscure the origin of illicit funds.

**Bank**

A subject obtained a modest loan with structured monthly repayments. Shortly after receiving the funds, the subject made multiple large repayments in cash that were well above the agreed instalment amount. After settling the loan early, the subject applied for a significantly larger loan within a short span. The unusual loan repayment behaviour followed by a rapid request for a significantly larger loan, was a red flag.



**E-Money**

An account was used to receive funds later confirmed as proceeds of fraud. The sender had been deceived into transferring money after engaging with a fake property rental listing, complete with fabricated documentation. After funds were received, they were swiftly moved to another bank account and withdrawn via ATM. The account holder became uncontactable thereafter.

This behaviour may be indicative of money mule activity and consistent with the placement and layering stages of money laundering.





**Legal**

A legal services firm was engaged for the purchase of a high-value property where, despite a lack of clear links between the buyer and sellers, the sellers displayed unusual urgency and changed legal representation mid-process; due diligence revealed that one of the sellers had a history of serious financial crimes, and the property, originally acquired at a significantly lower price, was now listed at a markedly inflated value, presenting a clear red flag for potential money laundering through real estate.



**Gaming**

A user employed a low-margin, minimal-risk betting strategy generating small but consistent profits, which were systematically withdrawn to a separate account from the one used for deposits. This activity/ behaviour presents a red flag as it may indicate an attempt to create a façade of legitimate gambling activity to layer illicit funds and obscure their origin.

**Gaming**

An account received large deposits with minimal wagering activity, while the user attempted numerous transactions using a high volume of different payment cards via a third-party processor. Combined with suspicious withdrawal patterns and card usage, this behaviour presents a red flag indicative of potential account misuse for money laundering purposes.



**VASP**

A VASP account was opened and verified via video call, with initial access matching the declared location. However, subsequent logins originated from multiple distant IP addresses, and the account activity, characterised by small deposits quickly converted to digital assets and immediately withdrawn via a blockchain network. This activity presents a red flag consistent with potential obfuscation tactics and money laundering through virtual assets.

**VASP**

A VASP account was used to receive cryptocurrency suspected of being linked to fraud conducted via crypto ATMs, with the funds being rapidly converted and distributed across multiple bank accounts associated with an organised network. It presented a red flag for potential money laundering and the use of cryptocurrency to facilitate illicit financial activities.





Gibraltar Financial Intelligence Unit  
HM Government of Gibraltar

**@gibfiu**  
**Suite 945 | Europort | Gibraltar**  
**[www.gfiu.gov.gi](http://www.gfiu.gov.gi)**