



Gibraltar Financial Intelligence Unit

HM Government of Gibraltar



SECTORAL TYPOLOGIES REPORT

A focus on trends and insights:

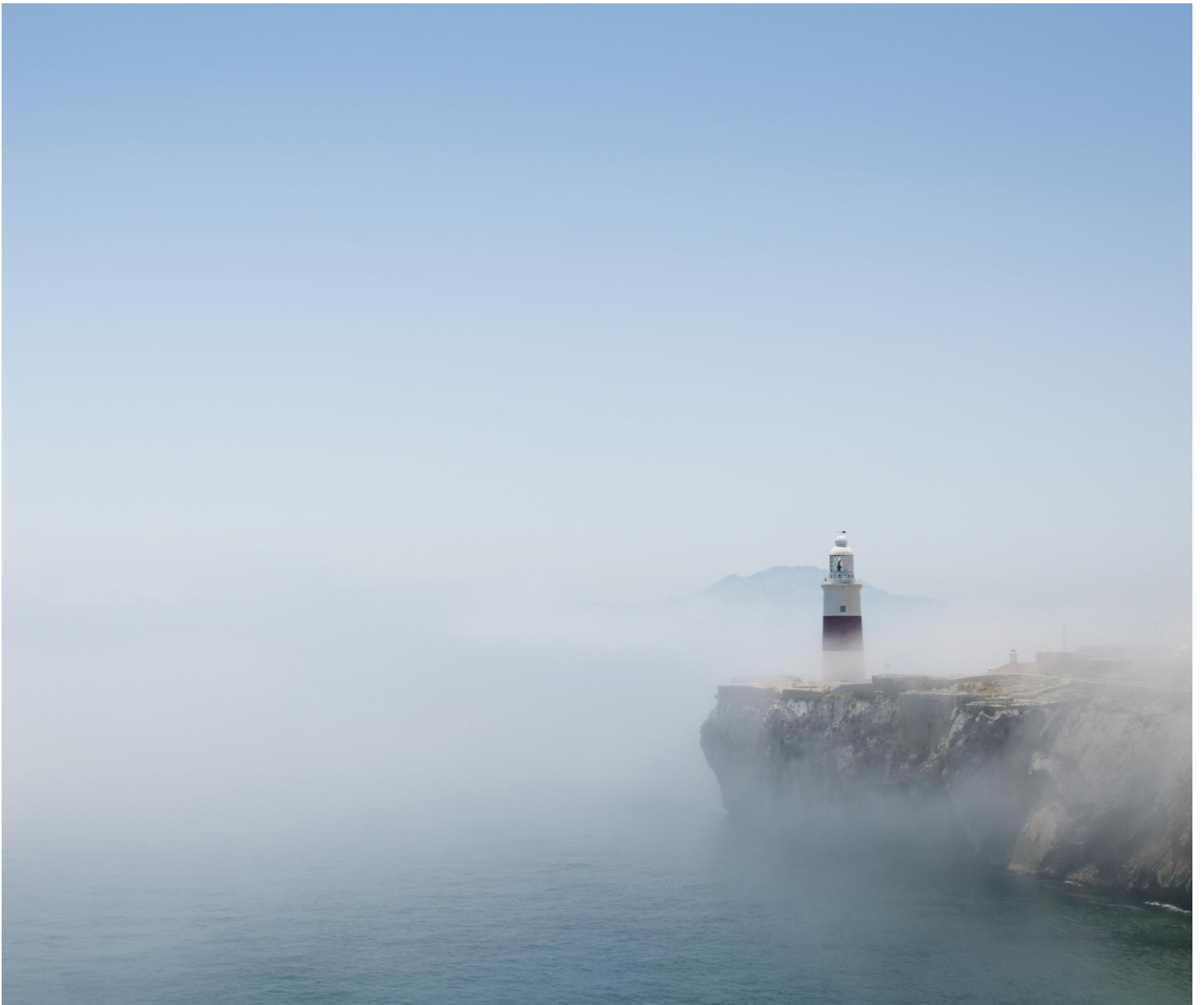
2018 - 2020

Contents

Introduction	3
Key red flag indicators across all sectors	6
Gaming Sector	19
E-money Sector	29
Distributed Ledger Technology Sector	39
Banking Sector	48
Trust and Corporate Services Providers Sector	58
Insurance Sector	67
Investment/ Fund Managers/ Securities Sector	78
Accountants, Auditors and Insolvency Practitioners Sector	86
Money Service Businesses and Money Value Transfer Services Sector	93
Legal Professionals and Notaries Sector	100
Real Estate Agents Sector	109
High Value Dealers and High Risk Dealers Sector	115



Introduction





BACKGROUND AND PURPOSE OF THE REPORT

As part of the work undertaken by the Gibraltar Financial Intelligence Unit (“GFIU”) towards addressing the recommendations made by Moneyval in December 2019, an extensive data analysis exercise was undertaken. This related to the analysis of Suspicious Activity Reports (“SARs”) received during the period January 2018 – December 2020, in order to develop sector specific Money Laundering typologies often encountered in Gibraltar. This data will support future National Risk Assessments (“NRA”).

The GFIU have undertaken detailed analyses of available SARs in order to achieve the following outcomes:



to synthesise current knowledge



to systematically assess the vulnerabilities of each relevant sector to involvement in Money Laundering and terrorist financing



to explore whether red flag indicators can be identified so as to enable Money Laundering Reporting Officers (“MLRO”) to distinguish and identify potentially criminal transactions from legitimate ones

Note 1: The SAR is a report submitted to the GFIU with information, which alerts law enforcement that certain client/customer or related business activity is in some way suspicious, and might indicate Money Laundering or financing of terrorism. Also known as a ‘disclosure’ and can refer to any information acquired by the reporter in the course of business deemed suspicious and of potential interest to Law Enforcement Agencies. Another recognised form of referring to a SAR is ‘STR’ (Suspicious Transaction Report) but GFIU will refer to it as a SAR throughout this document. The term ‘disclosure’ and ‘SAR’ are used interchangeably but both have the same meaning.

Note 2: A comprehensive guidance document for Terrorist Financing (“TF”) has been published by the GFIU, which contains sector specific red flags and indicators. While this Typologies Report is primarily designed to convey Money Laundering typologies, the GFIU advises that the TF Guidance document is used as a reference for TF related suspicions/ activities.

SECTORS IN SCOPE

The GFIU have identified the following relevant regulated sectors that have been scoped into this exercise and for each, a typologies report has been prepared:

- Gaming;
- E-Money;
- Distributed Ledger Technology (“DLT”);
- Banking;
- Trust and Corporate Services Providers (“TCSPs”);
- Insurance;
- Investment/Fund Managers/Securities;
- Accountants, Auditors and Insolvency Practitioners;
- Money Service Businesses (“MSB”) and Money Value Transfer Services (“MVTs”);
- Legal Professionals and Notaries;
- Real Estate Agents (“REA”); and
- High Value Dealers (“HVD”) and High Risk Dealers (“HRD”).



KEY OBJECTIVES

The key objectives of this report are:



To present the results of the data analysis exercise on a sector by sector basis in order to demonstrate the level of reporting from within each sector and the types of matter reported with a view to identifying red flag indicators;



To identify the total volume of SARs generated from within each sector in order to build a picture of the scale and extent of AML/CFT reported activity within Gibraltar;



Identify and highlight the specific types of transactions for which suspicious activity is reported in order to build sector specific typologies;



Present various sector specific case studies, with a view to demonstrate sector specific vulnerabilities and identify some of the most common red flag indicators;



Highlight some of the key challenges faced by the GFIU when analysing SARs, and highlight good practices in terms of the quality of the SARs received in order to provide sector specific guidance.



Key red flag indicators across all sectors





01

GAMING SECTOR RED FLAG INDICATORS

- Minimal or very low risk gambling activity. Substantial amounts deposited in various deposits and subsequent withdrawal of most of the funds within a short period;
- Chip dumping;
- Source of funds not provided as client has self-excluded himself;
- Funds deposited with suspected stolen cards or without authorisation of the cardholder;
- Use of suspected stolen funds from employer or from vulnerable people such as residents in care homes;
- Deposits from businesses with the suspicion of tax evasion;
- Deposits and/or source of funds from individuals others than the client; and
- A level of deposits inconsistent with the client's established profile.



02

E-MONEY SECTOR RED FLAG INDICATORS

- Initial registration of an account from one jurisdiction but subsequent logins into the account and withdrawals of funds in a high risk jurisdiction;
- Deposits into accounts from an account in the name of the client and subsequent withdrawal into other account(s) in the name of the client;
- Creation of multiple accounts for different clients from the same IP address, device and with common passwords;
- Receipt of funds where the name of the payee is different to that of the registered client;
- Deposit into the account from vouchers and subsequent cash withdrawal via ATM; and
- Funds received from clients account with an associated VASP and subsequent payment to a third party.



03

DLT SECTOR RED FLAG INDICATORS

- Clients conducting large initial deposits to open a new relationship with a DLT firm which are inconsistent with their client profile (employment, evidence of source of wealth, age etc.);
- Incomplete or insufficient KYC information provided, or a client declines requests for KYC documentation or ignores inquiries regarding source of funds to support deposits;
- A client has inadequate knowledge or provides inaccurate information about the transaction, the source of funds, or the relationship with the counterparty;
- A client provides forged documents or has edited photographs and/or identification documents as part of the on-boarding process; and
- A client purchases large amounts of Virtual Assets not substantiated by available wealth or consistent with their historical financial profile, which may indicate Money Laundering, a money mule, or a fraud victim.



04

BANKING SECTOR RED FLAG INDICATORS

- Potential new clients are reluctant to provide identity details, disclose source of funds or cooperate in any way;
- Inconsistencies in the information provided by clients pertaining to their business or personal activities and source of wealth;
- Clients trying to rush through transactions without providing the requested additional documentation which may be required;
- Clients are unable to explain their source of funds satisfactorily or provide contradictory statements;
- Clients who offer false or fraudulent identification, whether evident from the documents alone, from its lack of connection to the client or from its context in relation to other documents (e.g. use of ID or documents issued in other names without reasonable explanation);
- Clients attempt to obscure the beneficial ownership of assets. Due diligence could be provided for a front company with the aim for this to be used as a legitimate business to hide criminal activity and create legitimate funds;
- Clients who wish to maintain a number of trustees or clients' accounts that do not appear consistent with their type of business;
- Clients provide false/misleading explanations for due diligence purposes;
- Clients become uncontactable when requests for due diligence are made or questions are posed to them;
- Due diligence provided indicates a potential PEP which had not previously been identified;
- Unrealistic turnover or balances detected upon review of company financial statements; and
- Frequent changes to the account address or authorised signatories.



05



TCSP SECTOR RED FLAG INDICATORS

- Searches on a client or associate show, for example, adverse media attention, disqualification as a director, convictions for dishonesty or association with bribery in relation to contract procurement;
- Searches indicate connections to politically exposed persons or their family members which were not disclosed;
- Where the client is, or appears to be, acting on behalf of another person, an unwillingness to give the names of the persons they represent;
- The person acting as a director or representative does not appear to be a suitable representative or does not appear to have the expertise that the role requires;
- Frequent changes in ownership, officers, beneficiaries or trustees in an attempt to evade detection of any potential adverse information available;
- Client unwilling or refusing to provide information including documentary proof of himself or the beneficial owners of trusts or companies;
- Client carries out transactions for themselves or on behalf of the company that does not correspond with their background;
- The beneficial ownership is veiled in complexity making it impossible to determine;
- The client is secretive about the reasons for the way a company structure is being set up;
- The client's main business rationale is to engage with jurisdictions with, for example, weak anti Money Laundering laws or controls, limited corporate registration requirements, where there is no requirement to update ownership changes, limited beneficial ownership information requirements; and
- The client favours legal entities that are not transparent.



06

INSURANCE SECTOR RED FLAG INDICATORS

- Potential new clients are reluctant to provide identity details, disclose source of funds or cooperate in any way;
- Inconsistencies in the information provided by clients pertaining to their business or personal activities and source of wealth;
- Policyholder appears to have no legitimate interest in the insured risk, and policies are entered into without an economic rationale for doing so;
- Individuals seeking to pay large “top-ups” into an existing life insurance policy;
- Purchasing a general insurance policy, then making a claim soon after;
- Where the client appears more interested in learning about cancellation terms rather than about the benefits of the policy;
- Policies cancelled shortly after initiation, especially during the cooling-off period; and
- Individual attempts to seek out insurance for a property or vehicle which does not fit their economic profile.



07



INVESTMENT/FUND MANAGERS/SECURITIES RED FLAG INDICATORS

- Searches on a client or associate show, for example, adverse media attention, disqualification as a director, convictions for dishonesty or association with fraudulent schemes;
- Searches indicate connections to politically exposed persons or their family members which were not disclosed;
- Where the client is, or appears to be, acting on behalf of another person, an unwillingness to give the names of the persons they represent;
- The person acting as a director or representative does not appear to be a suitable representative or does not appear to have the expertise that the role requires;
- Frequent changes in ownership, officers, beneficiaries or trustees in an attempt to evade detection of any potential adverse information available;
- Client unwilling or refusing to provide information including documentary proof of himself or the beneficial owners;
- Client carries out transactions for themselves or on behalf of the company that does not correspond with their background;
- The client is secretive about the reasons and way a company structure is being set up;
- The client's main business rationale is to engage with jurisdictions with, for example, weak anti Money Laundering laws or controls, limited corporate registration requirements, where there is no requirement to update ownership changes, limited beneficial ownership information requirements;
- The client engages in investment decisions with no clear business rationale;
- The client engages in activity considered unusual when compared to their normal activity;
- The client provides inconsistent information such as multiple tax identification numbers, authorisation details or unverified documents;
- The client provides investment documentation which is deemed to be potentially fraudulent; and
- The client attempts to withdraw or release funds with immediacy, or in a timescale considered out of the normal ranges for these types of transactions.



08

ACCOUNTANTS, AUDITORS AND INSOLVENCY PRACTITIONER SECTORS RED FLAG INDICATORS

- Potential new clients are reluctant to provide identity details, disclose source of funds or cooperate in any way;
- Inconsistencies in the information provided by clients pertaining to their business or personal activities and source of wealth;
- Clients trying to rush through transactions without providing the requested additional documentation which may be required;
- Clients are unable to explain their source of funds satisfactorily or provide contradictory statements;
- Clients who offer false or fraudulent identification, whether evident from the documents alone, from its lack of connection to the client or from its context in relation to other documents (e.g. use of ID or documents issued in other names without reasonable explanation);
- Clients attempt to obscure the beneficial ownership of assets. Due diligence could be provided for a front company with the aim for this to be used as a legitimate business to hide criminal activity and create legitimate funds;
- Clients who wish to maintain a number of trustees or clients' accounts that do not appear consistent with their type of business;
- Clients provide false/misleading explanations for due diligence purposes;
- Clients become uncontactable when requests for due diligence are made or questions are posed to them;
- Due diligence provided indicates a potential PEP which had not previously been identified;
- Unrealistic turnover or balances detected upon review of company financial statements, that is not in line with the information held by the TCSP on the activity of the client; and
- Frequent changes to the account address or authorised signatories.



09

MSB & MVTS SECTOR RED FLAG INDICATORS

- Client who provides insufficient or suspicious information;
- Client who offers false identification, whether evident from the document alone, from the document's lack of connection to the client, or from the document's context with other documents (e.g., use of identification cards issued by different countries);
- Client who has been the subject of sanctions, known to the MVTS provider;
- Client whose transactions and activities indicate connection with potential criminal involvement or typologies or red flags provided in reports produced by FATF or competent authorities (e.g., the GFIU, the GFSC or the Royal Gibraltar Police) and client whose transaction patterns appear consistent with generation of criminal proceeds;
- Client who transfers funds to or from high risk jurisdictions;
- Activity inconsistent with client's business; and
- Unusual patterns of transactions.



10

LEGAL PROFESSIONALS AND NOTARIES SECTOR RED FLAG INDICATORS

- Searches on a client or associate show, for example, adverse media attention, disqualification as a director, convictions for dishonesty or association with bribery in relation to contract procurement;
- Searches indicate connections to politically exposed persons or their family members which were not disclosed;
- Where the client is, or appears to be, acting on behalf of another person, an unwillingness to give the names of the persons they represent;
- The person acting as a director or representative does not appear to be a suitable representative or does not appear to have the expertise that the role requires;
- Frequent changes in ownership, officers, beneficiaries or trustees in an attempt to evade detection of any potential adverse information available;
- Client unwilling or refusing to provide information including documentary proof of himself or the beneficial owners of trusts or companies;
- Client carries out transactions for themselves or on behalf of the company that does not correspond with their background;
- The beneficial ownership is veiled in complexity making it impossible to determine;
- The client is secretive about the reasons for and way a company structure is being set up;
- The client's main business rationale is to engage with jurisdictions with, for example, weak anti Money Laundering laws or controls, limited corporate registration requirements, where there is no requirement to update ownership changes, limited beneficial ownership information requirements; and
- The client favours legal entities that are not transparent.



REA SECTOR RED FLAG INDICATORS

- Clients with relationships identified by credible sources as providing funding or support for terrorist activities or that have terrorist organisations operating within them;
- Clients with relationships identified by credible sources as having significant levels of crime, corruption including illegal drugs, human trafficking, smuggling, illegal gambling etc.;
- Clients with relationships to countries subject to sanctions, embargoes etc.;
- Clients with relationships identified by credible sources as having weak governance, law enforcement and regulatory regimes;
- PEPs and persons closely associated with or related to PEPs who are considered as higher risk clients;
- Clients wanting to conduct or conducting their business in unusual or unconventional circumstances (when compared to known behaviours);
- Clients that are cash intensive businesses or wish to purchase real estate exclusively in cash;
- Clients who rely solely on the use of intermediaries to attempt to hide involvement;
- Clients who appear to actively and inexplicably avoid face-to-face meetings or who provide instructions intermittently without legitimate reasons;
- Searches on a client show, for example, adverse media attention, disqualification as director, convictions of dishonesty etc.;
- Clients who request that transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation for accelerating the transaction;
- Clients whose source of funds cannot be verified or is not in keeping with their known client profile;
- Clients are unable or reluctant to provide information about the source of funds or wealth when this is requested;
- Ownership of property is to be through a series of complex legal structures or complex corporate structures for no apparent reason;
- Client requests that the asking price/letting price be unreasonably higher than the valuation suggests;
- Client lets at or sells at a price which is significantly above or below market price, or a transaction which seems uneconomic or inefficient;
- Successive sale transactions, especially of the same property, in a short period of time with unexplained changes in value;
- Clients seeking to acquire property with no apparent legal, tax, business, economic or other legitimate reason; and
- Suspicions held over fraudulent transactions or transactions improperly accounted for etc.



12



HVD AND HRD SECTOR RED FLAG INDICATORS

- Cash payments from individuals residing in high-risk jurisdictions which may be more likely to be linked to Money Laundering;
- Cash payments received from clients operating in countries who restrict the use of cash and/or have limits in place for amounts of cash permitted to enter/leave the country;
- Does the transaction make commercial sense? Does the client have a market place for the goods you are selling in their home country?;
- Clients wanting to conduct or conducting their business in unusual or unconventional circumstances (when compared to known behaviours);
- Clients that are cash intensive businesses or wish to purchase goods exclusively in cash;
- Clients who rely solely on the use of intermediaries to attempt to hide involvement;
- Clients who appear to actively and inexplicably avoid face-to-face meetings or who provide instructions intermittently without legitimate reasons for their purchases;
- Clients seeking to pay for goods exclusively in other currencies such as euros with no area or business links to other jurisdictions;
- Clients who request that transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation for accelerating the purchase;
- Client whose source of funds cannot be verified or is not in keeping with their known client profile;
- Uncharacteristic transactions which are not in keeping with the client's financial situation; and
- The pattern and or frequency of an existing client has changed since the business relationship was established.



Gaming Sector





BACKGROUND TO THE SECTOR

Gibraltar has a closely regulated Gaming sector consisting mainly of remote gambling operators in the Business to Consumer (“B2C”) and Business to Business (“B2B”) sectors with one casino licence holder operating two small land based casino premises and two betting premises. There are also a number of Gaming machines located in premises (such as bars and restaurants) throughout Gibraltar.

As such, the residual risk present in all the gambling scenarios in Gibraltar, particularly online gambling is related primarily to user-related Money Laundering in which proceeds of a crime are used to gamble (e.g. theft from employer/ proceeds of fraud etc.). Whilst theft and fraud cases are only a very small percentage of the total relative size of active client numbers, nevertheless the risk of operators accepting deposits from the proceeds of crime is a crystallised risk which should be mitigated by effective ongoing client monitoring and due diligence.

The Gaming sector with its large client base is the largest SARs contributor over the period.

The NRA 2020 rated the Money Laundering threat of online Gaming as significant. Given its non-face to face nature, remote Gaming has inherent risk factors, which lead to this classification.

These factors include:

- Gaming clients are not required to physically be present for due diligence verification;
- Multiple online accounts could be set up to bypass controls in place;
- Clients from high risk jurisdictions may attempt to use VPNs or remote facilities to attempt to launder the proceeds of crime; and
- E-wallets used to source Gaming funds and winnings can make it difficult for operators to identify source of funds.

The NRA 2020 rated the Money Laundering threat of the Gaming sector as follows:

- Medium Low Risk for Remote Gambling;
- Medium Low Risk for Land-based Casinos;
- Medium Low Risk for Betting (land-based); and
- Low Risk for Bingo, Lotteries, Poker and Gaming Machines.



RESULTS OF DATA ANALYSIS

The data analysis exercise was undertaken in order to analyse the SARs submitted by entities within the Gaming sector during the years January – December 2018, 2019 and 2020.

The results have been included below.

Number of regulated Gaming companies within the sector

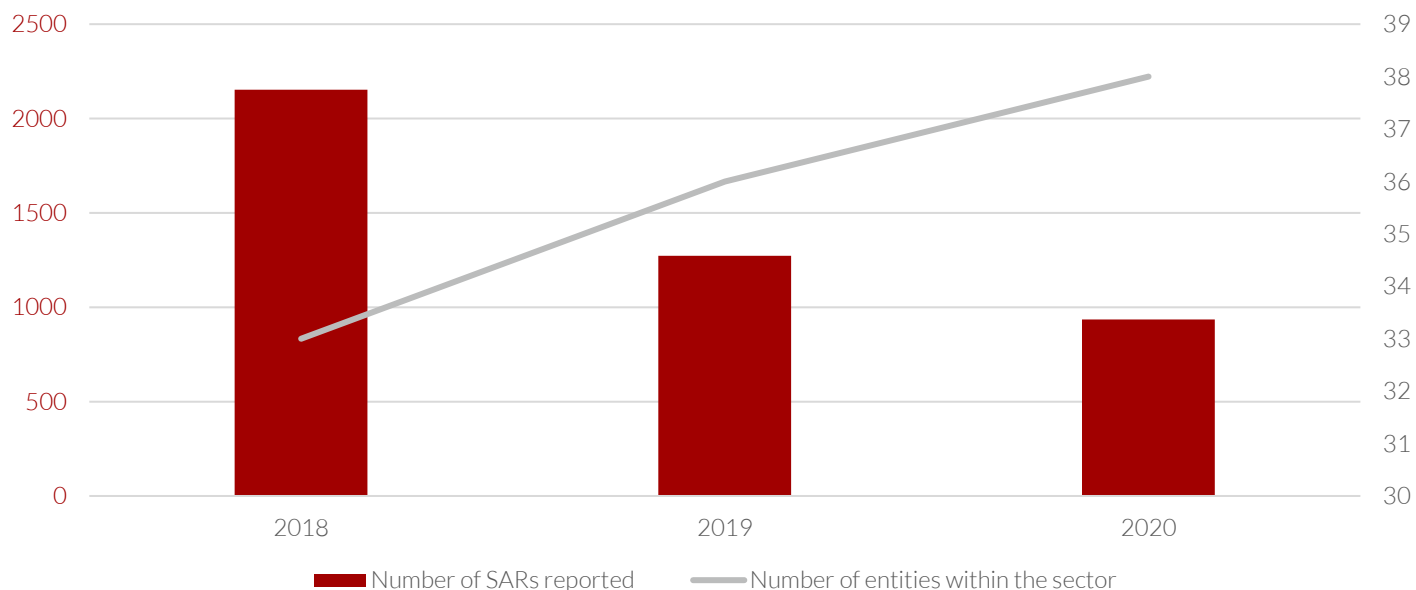
	2018	2019	2020
B2B Gaming entities	17	19	20
B2C Gaming entities	16	17	18
Total Gaming entities	33	36	38

Number of SARs received per regulated Gaming Company

Gaming entity	2018		2019		2020	
	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported
Gaming Entity 1	1487	69.10%	652	51.22%	184	19.66%
Gaming Entity 2	405	18.82%	235	18.46%	289	30.88%
Gaming Entity 3	94	4.37%	117	9.19%	121	12.93%
Gaming Entity 4	75	3.49%	129	10.13%	121	12.93%
Gaming Entity 5	22	1.02%	27	2.12%	27	2.88%
Gaming Entity 6	21	0.98%	13	1.02%	12	1.28%
Gaming Entity 7	10	0.46%	3	0.24%	17	1.82%
Gaming Entity 8	22	1.02%	18	0.47%	26	2.78%
Gaming Entity 9	6	0.28%	19	1.49%	25	2.67%
Gaming Entity 10	1	0.05%	27	2.12%	8	0.85%
Gaming Entity 11	3	0.14%	12	0.94%	2	0.21%
Gaming Entity 12	6	0.28%	3	0.24%	2	0.21%
Gaming Entity 13	-	-	16	1.26%	95	10.15%
Gaming Entity 14	-	-	1	0.08%	-	-
Gaming Entity 15	-	-	1	0.08%	4	0.43%
Gaming Entity 16	-	-	-	-	1	0.11%
Gaming Entity 17	-	-	-	-	1	0.11%
Gaming Entity 18	-	-	-	-	1	0.11%
Total	2152	100%	1273	100%	936	100%



Number of SARs reported vs Number of entities within the Sector



During 2018 – 2020, there has been a decrease in the number of Gaming companies reporting SARs, with 2018 seeing over 69% of the total SARs reported by a single entity. There was an overall slight increase in the number of licensed Gaming entities during the periods analysed and a significant decreasing trend in the number of SARs reported overall within the sector. This will be partly attributable to business relocating outside Gibraltar.

The number of SARs reported are highly concentrated within the reporting of five Gaming entities.

Some of the Gaming companies are online bingo and lottery betting operators, which are considered low risk as they do not have high value gamblers or are a fairly recent start-up, so it would not be surprising not too see many SARs submitted.

It should be noted that about half of the Gaming entities are B2B so the expectation for submission of SARs by these entities would be low numbers.

Top five entities in terms of SAR reporting

Gaming entity	2018		2019		2020	
	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported
Gaming Entity 1	1487	69.10%	652	51.22%	184	19.66%
Gaming Entity 2	405	18.82%	235	18.46%	289	30.88%
Gaming Entity 3	94	4.37%	117	9.19%	121	12.93%
Gaming Entity 4	75	3.49%	129	10.13%	121	12.93%
Gaming Entity 5	22	1.02%	27	2.12%	27	2.88%
Total	2083	96.8%	1160	91.12%	742	79.27%



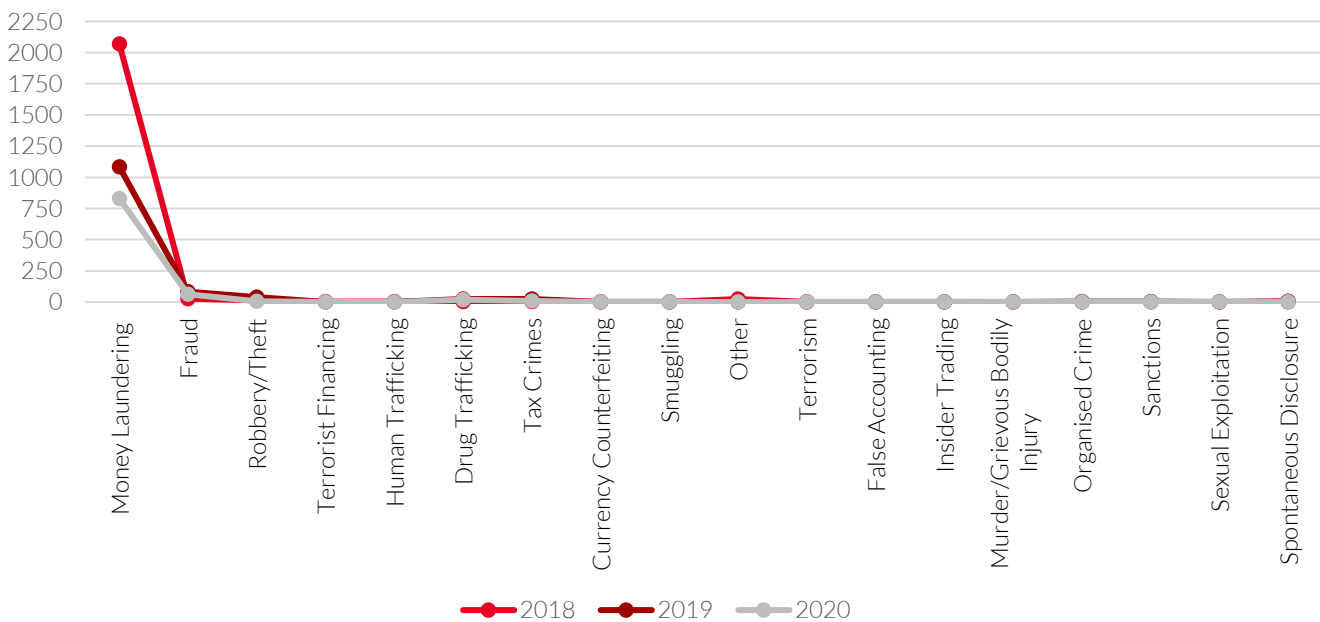
The number of SARs received from the remaining entities are minimal by comparison and raise various questions as to the identification and reporting of potentially suspicious behaviour by the Gaming industry.

- Is there a trend for SARs being filed in “defence” by certain Gaming entities? For example, is there a generally held view by some MLROs that it is better to report a particular type of SAR, and is this driven by compliance concerns instead of genuine suspicions?
- Are MLROs submitting SARs in respect of all internal suspicions raised or are they analysing and discarding some as not requiring submission?
- Is there evidence of certain types of potentially suspicious behaviour reported by certain companies that are not reported by others in the sector?
- Is there an apparent trend for specific crime typologies within the sector?
- Is there a failure by certain Gaming firms to identify and/or report suspicious activities?
- Perhaps some certain Gaming firms more susceptible to being used for criminal activity?

Of importance to note and particular to the Gaming industry, is the requirement for any SARs relating to UK clients should be reported to both the GFIU and the UK Financial Intelligence Unit (“UKFIU”). These reports are more likely to be of value to UK law enforcement who are capable of linkage with other UK law enforcement intelligence. The requirement goes further and these SARs should be submitted simultaneously with no undue delay.

In order to present findings to the above questions, further data analysis was undertaken.

Number of SARs reported by principal suspected criminality



Overwhelmingly, the data above demonstrates that Money Laundering is the dominant suspected criminality reported by MLROs within the Gibraltar Gaming sector. Whilst Fraud, Robbery/Theft, Drug Trafficking and Tax Crimes have been reported and experienced increases in suspected occurrence during 2019 and 2020, crimes relating to suspected Money Laundering represent the majority of SARs disclosed within the local Gaming community.



There will be SARs where there are multiple suspected criminalities. Themis works on a 'principal crime system', which means that in cases which contain more than one type of offence, it will record the principal suspected criminality. As this is a subjective assessment, there may be inconsistencies between MLROs. There are instances where MLROs have more information than what is included within the SAR, which determines what suspected criminality they record. When there are high risk criminalities like Terrorist Financing, Sexual Exploitation, etc. involved, these should always be recorded as the suspected criminality.

This raises further questions as to whether Money Laundering has been selected as a default suspected criminality, when there may be more appropriate and relevant categories, which would further enhance the quality of the reports received by the GFIU and allow for more efficient review and analysis.

GROUNDINGS FOR SUSPICION

As is the case with suspected criminality, there are SARs which have multiple grounds for suspicion. During the operational analysis of the SAR, the GFIU will record the principal grounds for suspicion. The GFIU's internal Themis system is designed to select one 'grounds for suspicion' category which provides a more comprehensive presentation of statistical data in line with international standards of recording data. However, although some SARs may appear similar, an in depth analysis of each SAR will determine the most appropriate grounds for suspicion to be recorded.

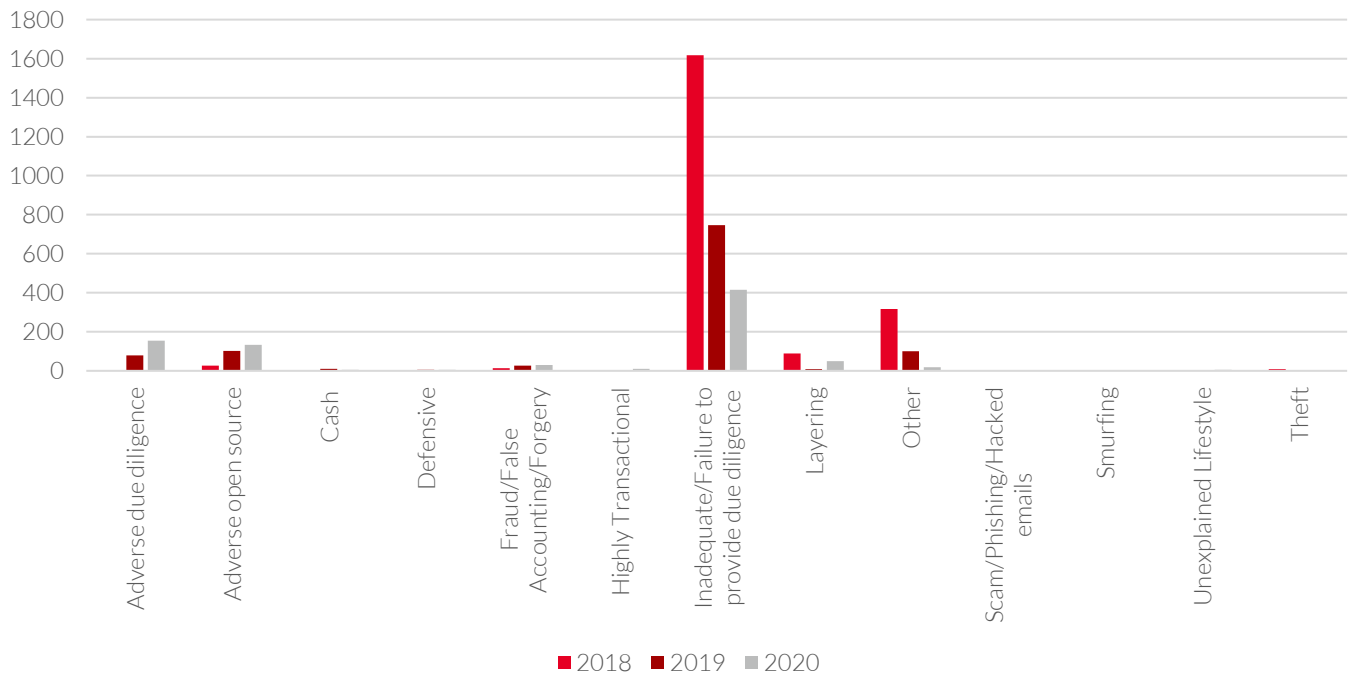
The narrative of the SAR will include all the grounds for suspicion and these are searchable by key words.

As the majority of SARs reported relate to suspected money-laundering offences as detailed above, further data analysis was undertaken to provide insights into the grounds for suspicion that resulted in SAR disclosures.



MONEY LAUNDERING

SARs raised by principal grounds of suspicion - Money Laundering



The majority of SARs raised were filed by MLROs due to perceived inadequate due diligence and/or failure to provide due diligence by individual clients. Adverse due diligence and adverse open source information were also reported in significant numbers. However, all other offences reported were immaterial in comparison to due diligence related SARs.

The receipt of due diligence occurs at different stages throughout a client relationship, beginning at the client onboarding stage, where an individual applies to become a client of the Gaming entity and provides initial personal identification details, such as their name, address, date of birth etc. This information should be verified by the Gaming entity using reliable and independent means such as databases, documents and other supplementary open source sources to confirm the identity of the individual in question. At this stage, dependent on the verification undertaken, should the Gaming Company not be able to verify the client’s identity, the client relationship may end, unless further documents to support verification are provided and accepted. There is some evidence of MLROs raising SARs at this stage before a deposit has been placed by a client (and any financial flow of funds has been undertaken). In addition, Gaming clients should be subject to Enhanced Due Diligence (“EDD”) before being allowed to place a deposit, and at various other stages through the client relationship lifecycle. EDD can take the form of additional identification checks and supplemental measures to verify or certify documents such as the source of wealth and funds that are deposited. In the circumstances where adverse and/or inadequate data is provided during the course of a client relationship, the data analysis demonstrates that MLROs within the Gaming industry will proceed to raise a SAR to notify the GFIU.



Number of SARs raised by regulated entity with principal grounds of suspicion recorded as inadequate/failure to provide due diligence

Gaming entity	2018			2019			2020		
	Number of SARs reported: due diligence	Total number of SARs reported	% number of due diligence SARs to total population	Number of SARs reported: due diligence	Total number of SARs reported	% number of due diligence SARs to total population	Number of SARs Reported: due diligence	Total number of SARs reported	% number of due diligence SARs to total population
Gaming Entity 1	1191	1487	80.09%	561	652	86.04%	165	184	89.69%
Gaming Entity 2	276	405	68.15%	35	235	14.89%	106	289	36.68%
Gaming Entity 3	56	94	59.57%	16	117	13.68%	9	121	7.44%
Gaming Entity 4	49	75	65.33%	96	129	74.42%	84	121	69.42%
Gaming Entity 5	12	22	54.55%	8	27	29.63%	12	27	44.44%
Gaming Entity 6	2	21	9.52%	-	13	-	1	12	8.33%
Gaming Entity 7	7	10	70.00%	2	3	66.67%	3	17	17.65%
Gaming Entity 8	11	22	50.00%	2	18	11.11%	1	26	3.85%
Gaming Entity 9	2	6	33.55%	19	19	100%	3	25	12.00%
Gaming Entity 10	1	1	100%	-	27	-	-	8	-
Gaming Entity 11	3	3	100%	2	12	16.67%	-	2	-
Gaming Entity 12	-	6	-	1	3	33.33%	-	2	-
Gaming Entity 13	-	-	-	4	16	25.00%	21	95	22.11%
Gaming Entity 14	-	-	-	-	1	-	-	-	-
Gaming Entity 15	-	-	-	-	1	-	1	4	25.00%
Gaming Entity 16	-	-	-	-	-	-	1	1	100%
Gaming Entity 17	-	-	-	-	-	-	-	1	-
Gaming Entity 18	-	-	-	-	-	-	-	1	-
Total SARs	1607	2152	74.67%	745	1273	58.52%	416	936	44.44%
Median	7	-	-	16	-	-	9	-	-



During 2018, there were six Gaming entities that reported SARs relating to due diligence above the median score. (2019: 4 Gaming entities, 2020: 5 Gaming entities) and these are largely proportionate to those entities that reported the highest number of SARs for both Money Laundering offences, and generally overall.

From the results of the data analysis above, it is apparent that a number of Gaming entities report consistently higher levels of receipt of inadequate due diligence or failure to provide due diligence as their grounds of suspicion. This suggests illicit spend rather than Money Laundering. Across the three years, one entity has accounted for the overwhelming majority of SARs raised. In relation to due diligence related SARs, the above have been reported to the GFIU because the Gaming entity has been “unable to verify source of funds.” Whilst the number of due diligence related SARs remain high across some of the other entities, the level of due diligence related SARs raised by this entity skew the results significantly.

SARs have been reported to the GFIU for suspicions such as:

- Minimal or very low risk gambling activity. Substantial amounts deposited in various deposits and subsequent withdrawal of most of the funds within a short period;
- Chip dumping;
- Source of funds not provided as client has self-excluded himself;
- Funds deposited with suspected stolen cards or without authorisation of the cardholder;
- Use of suspected stolen funds from employer or from vulnerable people such as residents in care homes;
- Deposits from businesses with the suspicion of tax evasion;
- Deposits and/or source of funds from individuals others than the client; and
- A level of deposits inconsistent with the client’s established profile.



Defensive SARs

	2018		2019		2020	
	Yes	No	Yes	No	Yes	No
GFIU conclusion						
Defensive SAR	25	2127	258	1014	139	797

As described earlier in the chapter, the data analysis undertaken aimed to assess whether there was a culture of defensive SARs submitted to the GFIU by the Gibraltar Gaming sector. A defensive SAR arises where an activity or a transaction is deemed not suspicious upon further analysis by the GFIU. SARs are required to be filed when a transaction or an attempted transaction involve funds derived from any illegal activity, or when the transaction has no apparent lawful purpose. As the number of SARs received within the Gaming sector have decreased significantly over the analysed periods, the analysis above attempts to assess whether the number of defensive SARs raised has also decreased. Many entities are wary to be seen by both the GFIU and by their regulator as being complacent or soft on potential instances of Money Laundering. As regulatory and legal scrutiny has increased in this area, so has the risk of regulatory and reputational risk to these entities and so the high number of SARs deemed to have been filed in a defensive manner are likely to be explained by this. However, it is important to note that the sheer volume of additional workload created by these defensive SARs where no suspicious activity is contained within have a negative impact on the GFIU, and may even lead to a dilution on the value of SAR reporting as a whole.

Links to Politically Exposed Persons (“PEPs”)

	2018		2019		2020	
	Yes	No	Yes	No	Yes	No
GFIU conclusion						
Link to /PEP	-	2152	21	2226	8	928

The above analysis suggests that there is very little evidence of SARs raised by Gaming entities containing a link to a PEP. This is reported by the MLROs when raising a SAR and both regulations and legal frameworks within Gibraltar require that EDD be applied to all PEPs, including immediate family and known close associates. For any client deemed to be a PEP, specific approval must be obtained for the account opening to continue, the source of funds/wealth must be established and enhanced ongoing monitoring must be applied to the account.



02 E-money Sector





BACKGROUND TO THE SECTOR

Gibraltar has a small number of regulated E-money firms (for the purposes of this analysis, a bank, that provides E-money services, has been classified as an E-money firm, rather than a bank).

E-money is defined as electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for making payment transactions and which is accepted by a natural or legal person other than the electronic money issuer. A key characteristic of E-money is its pre-paid nature, which essentially means that an account, card or a device needs to be credited with a monetary value in advance of any spending.

Gibraltar's E-money firms offer a mix of both physical chip cards (similar to traditional debit cards) or software based applications, which allow for online spending. The firms offer both 'open loop' products, which can be used at any retailer or merchant, as well as at ATMs (if applicable), and 'closed loop' products, usually in the form of gift cards which can only be spent at specific merchants or retailers. Currently, all E-money firms passport their services into the UK and various EU jurisdictions and the E-money sector's client base is largely constituted from these jurisdictions, as opposed to a local client base.

Whilst there are a small number of E-money firms, the volume and value of financial transactions generated is substantial with Moneyval noting the largest client base standing at 2,291,113 individuals and 39,238 corporate clients, with a total E-money outstanding of GBP 225,526,315 (2018). With its large client base, the E-money sector is one of the largest SARs contributors over the periods analysed and the predominant predicate offence indicated in these SARs are "fraud" and "Money Laundering".

The NRA 2020 rated the Money Laundering threat of the E-money sector as follows:

- High risk for Open loop products (where cash is used to load E-money);
- Medium Low Risk for Open loop products (where bank accounts are used to load e-money); and
- Low Risk (for closed loop products).

Given its non-face-to-face nature, E-money has inherent risk factors, which lead to this classification.

These factors include:

- E-money clients are not required to physically be present for due diligence verification;
- Prepaid cards have been known to be used by terrorists in order to circumvent cash declarations required at border controls;
- Prepaid cards have become known as potential replacements for human money mules where stolen identities have been used to obtain cards which are then loaded with the proceeds of crime, and criminal funds laundered; and
- Prepaid cards have been used to fund human trafficking, including the collection of funds in exchange for trafficked individuals.



RESULTS OF DATA ANALYSIS

The data analysis exercise was undertaken in order to analyse the SARs submitted by entities within the E-money sector during the years January – December 2018 - 2020.

The results have been included below.

Number of regulated E-money firms within the sector

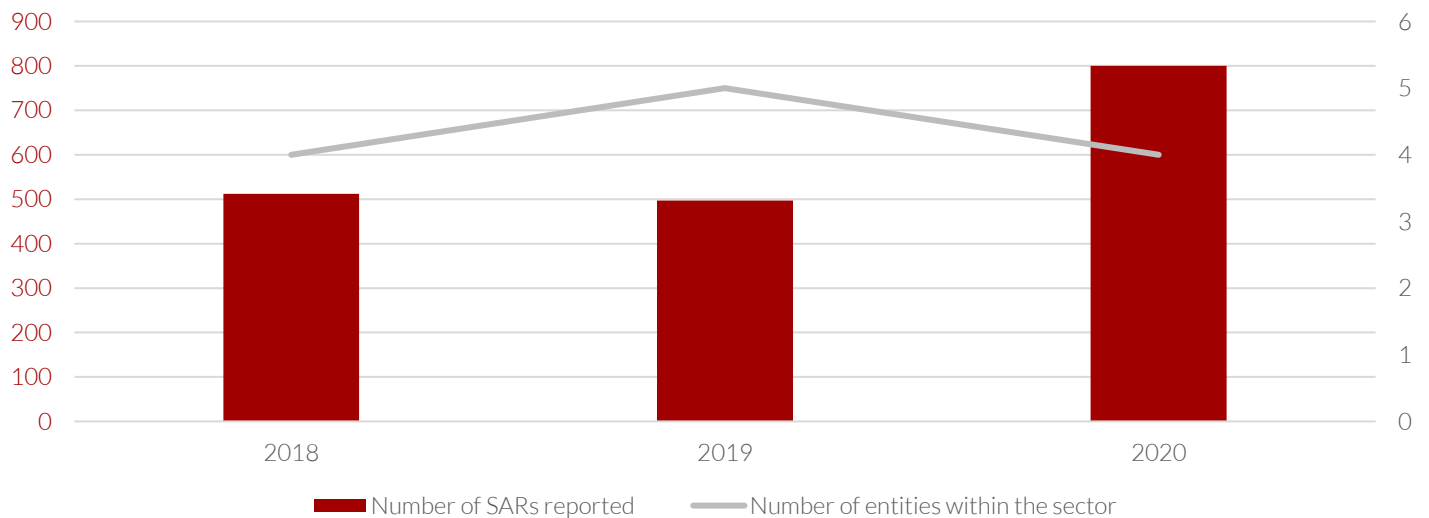
2018	2019	2020
4	5	4

Number of SARs received per regulated E-money firm

E-money firm	2018		2019		2020	
	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported
E-Money Entity 1	156	30.47%	217	43.66%	283	35.38%
E-Money Entity 2	103	20.12%	112	22.54%	126	15.75%
E-Money Entity 3	222	43.36%	166	33.40%	386	48.25%
E-Money Entity 4	29	5.66%	-	-	-	-
E-Money Entity 5	2	0.39%	2	0.40%	5	0.63%
Total	512	100%	497	100%	800	100%



Number of SARs reported v Number of Entities within the Sector



The number of SARs raised has substantially increased in 2020 after remaining relatively stable in 2018 and 2019. This generally represents an increase in SARs across all E-money firms. The number of SARs reported are highly concentrated within the reporting of three out of five of the licensed E-money firms. E-money firms might report SARs differently. Some SARs contain numerous subjects, whilst similar SARs may also be reported with numerous individual SARs with one subject. This can partially be attributed to internal investigations undertaken by some E-money firms, which link additional subjects to the principal subject.

Some E-money firms are associated to other E-money firms or VASPs. SARs are received where the suspicion was originally raised within these associated entities.

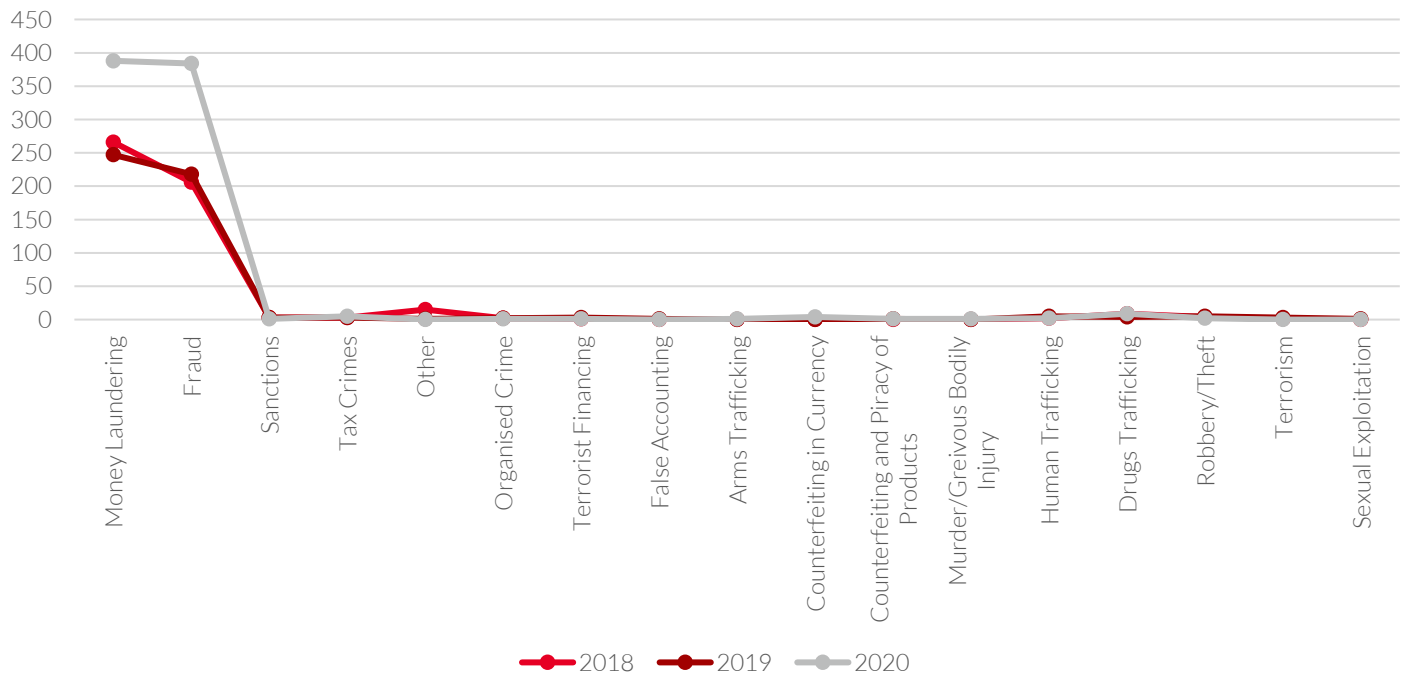
The number of SARs received from the remaining firms are minimal by comparison and raise various questions as to the identification and reporting of potentially suspicious behaviour within the industry.

- Is there a trend for SARs being filed in “defence” by certain E-money firms? For example, is there a generally held view by some MLROs that it is better to report a particular type of SAR, and is this driven by compliance concerns instead of genuine suspicions?
- Are MLROs submitting SARs in respect of all internal suspicions raised or are they analysing and discarding some as not requiring submission?
- Is there a prevalence of certain types of potentially suspicious behaviour occurring within the client base of some companies over others?
- Is there a failure by certain E-money firms to identify and/or report suspicious activities?
- Are some certain E-money firms or their services and products more susceptible to being used for criminal activity?

In order to present findings to some of the above questions, further data analysis was undertaken.



Number of SARs reported by suspected criminality



The data above demonstrates that Money Laundering and Fraud are the most prevalent suspected criminalities reported by MLROs within Gibraltar's E-money sector. There will be SARs where there are multiple suspected criminalities. Themis works on a 'principal crime system', which means that in cases which contain more than one type of offence, it will record the principal suspected criminality. As this is a subjective assessment, there may be inconsistencies between MLROs. There are instances where MLROs have more information than what is included within the SAR, which determines what suspected criminality they record.

When there are high risk criminalities like Terrorist Financing, Sexual Exploitation, etc. involved, these should always be recorded as the suspected criminality. There is a spread of suspicious behaviours reported and these have been analysed further below.

GROUNDS FOR SUSPICION

As is the case with suspected criminality, there are SARs which have multiple grounds for suspicion. During the operational analysis of the SAR, the GFIU will record the principal grounds for suspicion. The GFIU's internal Themis system is designed to select one 'grounds for suspicion' category which provides a more comprehensive presentation of statistical data in line with international standards of recording data. However, although some SARs may appear similar, an in depth analysis of each SAR will determine the most appropriate grounds for suspicion to be recorded.

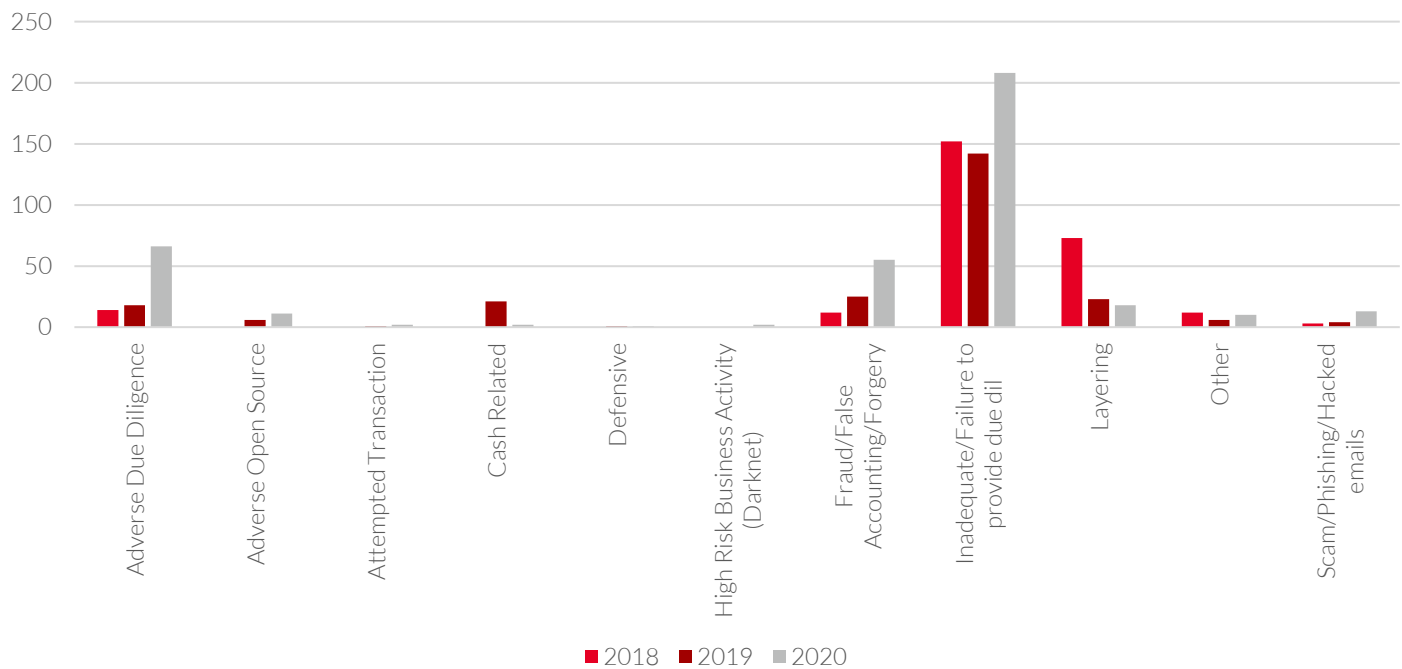
The narrative of the SAR will include all the grounds for suspicion and these are searchable by key words.

As the majority of SARs reported relate to suspected Money Laundering and fraud related offences as the principal recorded grounds for suspicion as detailed above, further data analysis was undertaken to provide insights into the grounds for suspicion that resulted in SAR disclosures. The below analysis is based on the principal recorded suspected criminality and grounds for suspicion.



MONEY LAUNDERING

SARs raised by principal grounds of suspicion - Money Laundering



The majority of SARs raised were filed by MLROs due to perceived inadequate due diligence and/or failure to provide due diligence by individual clients as the principal grounds for suspicion. Adverse due diligence and Fraud, False Accounting and/or Forgery were also highly reported.

The receipt of due diligence occurs at different stages throughout a client relationship, beginning at the client onboarding stage, where an individual applies to become a client of the E-money firm and provides initial personal identification details, such as their name, address, date of birth etc. Firms need to identify the client and then verify using a risk based approach. There is some evidence of MLROs raising SARs before a client has created E-money (and any financial flow of funds has been undertaken).

A feature of some E-money models is the reliance on distributors and agents involved in the delivery channel of E-money products. As the majority of the E-money firms' clients are non-Gibraltar based, a reliance on third parties is expected and these distributors and agents will market and offer the E-money products in their own local markets in partnership with the Gibraltar E-money firms. Oversight, therefore, of these outsourced partners is crucial in managing AML/CFT risks with E-money firms required to have effective oversight over these partners, and their activities at all times. Weaknesses in oversight by the E-money firms could lead to failures in the application of due diligence procedures by the third parties who may innocently or otherwise, accept fraudulent identity documentation, or allow the E-money products to be used for the layering of criminal funds. E-money firms are responsible for ensuring that their agents and distributors act in accordance with the requirements of our legislation and regulations and ensure this through monitoring, audits and oversight. From reviewing the SARs reported, it is also evident that SARs are being reported as part of the E-money firms' ongoing monitoring of its client base.



There is some overlap between the reporting of SARs, specifically Fraud related SARs. For some SARs, the grounds for suspicion is recorded as the receipt of inadequate due diligence or failure to provide due diligence and suspected crimes relating to Fraud/False Accounting/Forgery as Money Laundering related offences. However, for others SARs raising the same suspicions are recorded as Fraud related offences. Many of these SARs arise from a client's use of false identification documents, for example, or inadequate provision of evidence to support the source of funds being loaded as E-money. As was mentioned previously, only the principal grounds for suspicion are recorded in Themis, even though there may be multiple grounds. This is a subjective assessment of what is considered the most appropriate grounds to be recorded. An example is when the initial grounds is fraud due to a fraudulent payment which results in enhanced due diligence being requested but the client fails to provide this. Correctly recording the grounds of suspicion enhances the data analysis capabilities of the GFU.

In relation to Money Laundering related SARs, these have been reported to the GFU for suspicions such as:

- Initial registration of an account from one jurisdiction but subsequent logins into the account and withdrawals of funds in a high risk jurisdiction;
- Deposits into accounts from an account in the name of the client and subsequent withdrawal into other account(s) in the name of the client;
- Creation of multiple accounts for different clients from the same IP address, device and with common passwords;
- Receipt of funds where the name of the payee is different to that of the registered client;
- Deposit into the account from vouchers and subsequent cash withdrawal via ATM; and
- Funds received from clients account with an associated VASP and subsequent payment to a third party.

Number of SARs raised by regulated entity with the principal grounds of suspicion recorded as inadequate/failure to provide due diligence

E-money firm	2018			2019			2020		
	Number of SARs reported: due diligence	Total number of SARs reported	% number of due diligence SARs to total population	Number of SARs reported: due diligence	Total number of SARs reported	% number of due diligence SARs to total population	Number of SARs Reported: due diligence	Total number of SARs reported	% number of due diligence SARs to total population
E-Money Entity 1	111	156	71.15%	133	217	61.29%	184	283	65.02%
E-Money Entity 2	13	103	12.62%	7	112	6.25%	21	126	16.67%
E-Money Entity 3	37	222	16.67%	2	166	1.20%	1	386	0.26%
E-Money Entity 4	3	29	10.34%	-	-	-	-	-	-
E-Money Entity 5	-	2	-	-	2	-	2	5	40.00%
Total SARs	164	512	32.03%	142	497	28.57%	208	800	26.00%
Median	25	-	-	7	-	-	11	-	-

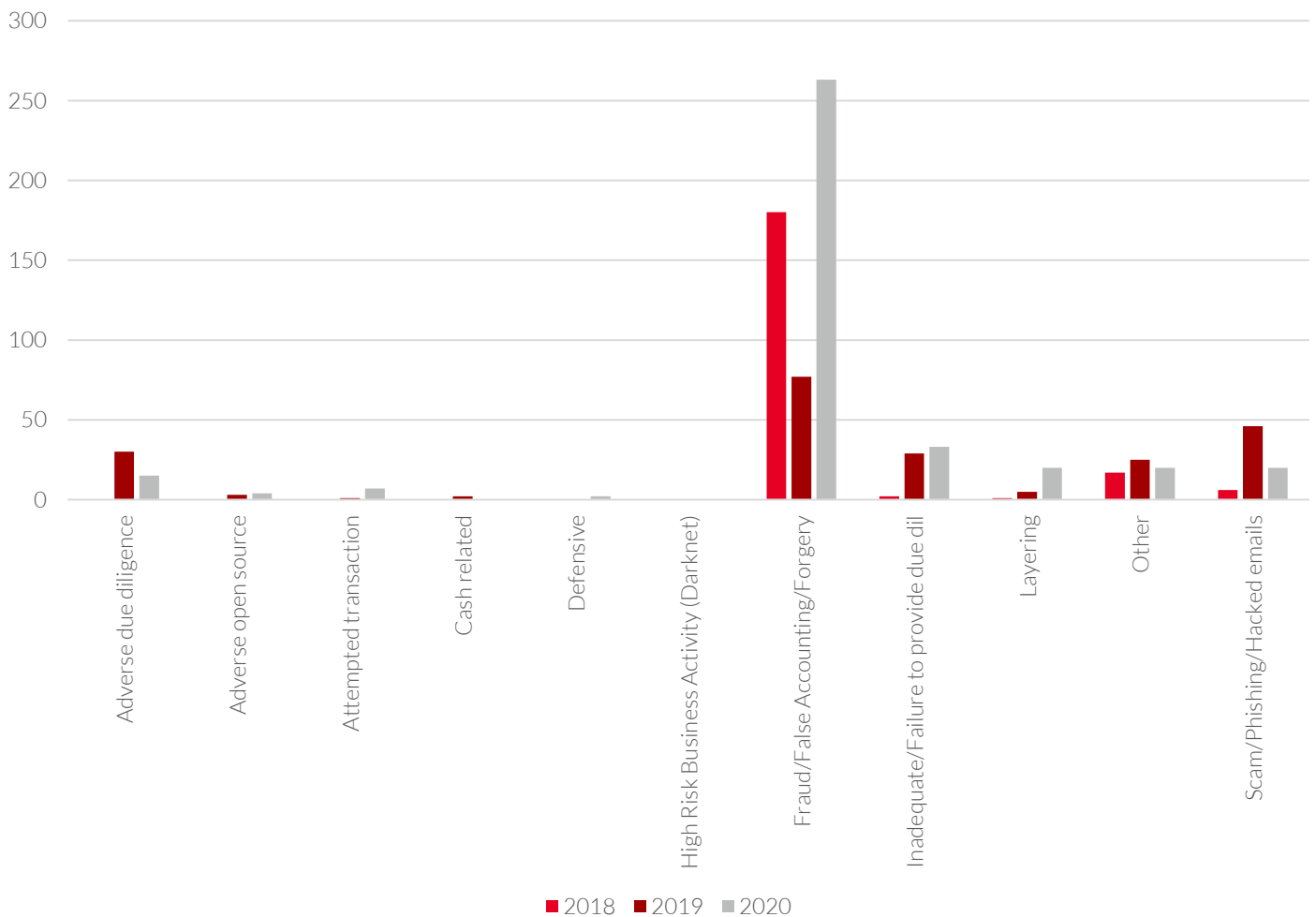


During 2018, there were two E-money firms which reported SARs relating to due diligence, above the median. (2019: 1 E-money firm, 2020: 2 E-money firms) and these are largely proportionate to those entities that reported the highest number of SARs for both Money Laundering offences, and generally overall.

From the results of the data analysis above, it is apparent that for an E-money firm consistently higher levels of receipt of inadequate due diligence or failure to provide due diligence is recorded as the principal grounds of suspicion. Across the three years, one has accounted for the overwhelming majority of SARs raised. In relation to due diligence related SARs, the above have been reported to the GFIU because the entity has been “unable to verify source of funds.” Whilst the number of due diligence related SARs remain high across another of the other entities, the level of due diligence related SARs raised by this entity skew the results significantly. Included further within the chapter are case studies relating to source of funds, which should provide further assistance to MLROs in helping them to assess when to report SARs pertaining to source of funds.

FRAUD

SARs raised by principal grounds of suspicion - Fraud





As detailed earlier in the chapter, there is an overlap in the grounds of suspicion recorded with Fraud, False Accounting, Forgery, Inadequate and/or failure to provide due diligence and adverse due diligence, being recorded as both Money Laundering and Fraud. The E-money firms also reported higher levels of SARs pertaining to Scams, Phishing or Hacked emails during the periods in question.

Number of SARs raised by regulated entity with principal grounds of suspicion recorded as Fraud/False Accounting/Forgery

E-money firm	2018			2019			2020		
	Number of SARs reported: Fraud/False Accounting/ Forgery	Total number of SARs reported	% number of due diligence SARS to total population	Number of SARs reported: Fraud/False Accounting/ Forgery	Total number of SARs reported	% number of due diligence SARS to total population	Number of SARs reported: Fraud/False Accounting/ Forgery	Total number of SARs reported	% number of due diligence SARS to total population
E-Money Entity 1	1	156	0.64%	6	217	2.76%	2	283	0.71%
E-Money Entity 2	48	103	46.60%	8	112	7.14%	23	126	18.25%
E-Money Entity 3	47	222	21.17%	63	166	37.95%	232	386	60.10%
E-Money Entity 4	7	29	24.14%	-	-	-	-	-	-
E-Money Entity 5	-	2	-	-	2	-	1	5	20.00%
Total SARs	103	512	20.12%	77	497	15.49%	258	384	67.19%
Median	27	-	-	8	-	-	13	-	-

Following a similar trend as reported in the Money Laundering analysis above, there are two E-money firms which reported Fraud related SARs above the median for the year 2018 (2019: 1 E-money firm, 2020: 2 E-money firms) and these are also largely proportionate to the entities that reported the highest volume of SARs during the periods analysed.

From the results of the data analysis above, it is apparent that an individual E-money firm consistently records higher levels of Fraud as the principal grounds of suspicion across the three years, and one firm has accounted for the overwhelming majority of SARs raised.

In relation to Fraud related SARs, these have been reported to the GFU for suspicions such as:

- The use of multiple and/or stolen credit cards to load E-money funds, including cards registered in a jurisdiction with no apparent link to the subject;
- Creation by client of both payer and payee accounts with stolen identities and credit cards with subsequent request for payment for goods and services from the payer account;
- COVID19 benefit fraud, with payments being received into the account from jurisdictions other than where the client is resident and/or the names in the description are different to that of the client;
- The use of E-money in relation to Ponzi Schemes;
- Unauthorised card loading (where third parties load funds onto cards rather than the authorised account owner); and
- The use of fraudulent or stolen identity documentation.



Whilst the number of due diligence related SARs remain high across another of the other entities, the level of Fraud related SARs raised by Entity 3 skew the results significantly. Included further within the chapter are case studies relating to fraud related SARs, which should provide further assistance to MLROs in helping them to assess when to correctly categorise SARs as fraud related.

Defensive SARs

	2018		2019		2020	
	Yes	No	Yes	No	Yes	No
GFIU conclusion						
Defensive SAR	3	509	99	411	37	763

As described earlier in the chapter, the data analysis undertaken aimed to assess whether there was a culture of defensive SARs submitted to the GFIU by the Gibraltar E-money sector. A defensive SAR arises where an activity or a transaction is deemed not suspicious upon further analysis by the GFIU. SARs are required to be filed when a transaction or an attempted transaction involve funds derived from any illegal activity, or when the transaction has no apparent lawful purpose. As the number of SARs received within the E-money sector have increased significantly over the periods analysed, the analysis above attempts to assess whether the number of defensive SARs raised has also increased. Many entities are wary to be seen by both the GFIU and by their regulator as being complacent or soft on potential instances of Money Laundering. As regulatory and legal scrutiny has increased in this area, so has the risk of regulatory and reputational risk to these entities and so the number of SARs deemed to have been filed in a defensive manner are likely to be explained by this. However, it is important to note that the volume of additional workload created by these defensive SARs where no suspicious activity is contained within have a negative impact on the GFIU, and may even lead to a dilution on the value of SAR reporting as a whole.

Links to Politically Exposed Persons (“PEPs”)

	2018		2019		2020	
	Yes	No	Yes	No	Yes	No
GFIU conclusion						
Link to PEP	1	5	4	493	1	799

The above analysis suggests that there is very little evidence of SARs raised by E-money firms containing a link to a PEP. This is reported by the MLROs when raising a SAR and both regulations and legal frameworks within Gibraltar require that EDD be applied to all PEPs, including immediate family and known close associates. For any client deemed to be a PEP, specific approval must be obtained for the account opening to continue, the source of funds/wealth must be established and enhanced ongoing monitoring must be applied to the account.



Distributed Ledger Technology Sector





BACKGROUND TO THE SECTOR

Gibraltar has a small but growing DLT sector which since January 2018, is authorised and regulated by the Gibraltar Financial Services Commission via principles driven regulatory framework.

DLT has developed growing usage within the financial services sector and Virtual Assets are one of the most popular use of DLT locally. Virtual Assets can be purchased and traded via Virtual Asset Service Providers (“VASP”) and it is the use of DLT for storing or transmitting value belonging to others, which is authorised and regulated locally. The locally developed framework is principles based and includes the requirement for systems to be in place within DLT firms for the prevention, detection and disclosure of financial crime risks such as Money Laundering and terrorist financing. This principle therefore introduces the requirement for DLT firms to collect valid KYC and verify the due diligence provided by clients. Transaction monitoring is also required in order to monitor and identify any potential patterns of suspicious behaviour, which should be reported to the GFIU.

The sector is highly concentrated amongst a small number of firms, however, it was one of the largest SARs contributors over the periods analysed and the predominant predicate offence indicated in these SARs are “fraud” and “Money Laundering”.

The NRA 2020 rated the Money Laundering threat of the DLT sector as follows:

- Medium High Risk for Wallet Providers;
- Medium Low Risk for Exchanges;
- Medium Low Risk for Initial Coin Offerings;
- Medium Low Risk for Over The Counter services; and
- Low Risk for Peer-to-Peer Lending.

The NRA explains that the full regulatory framework found in Gibraltar mitigates the inherent risks of the use of DLT technology in financial services, but also highlights the European Union’s Supranational Risk Assessment Report that shows that terrorist organisations may have an interest in utilising Virtual Assets to finance terrorist activities. For these reasons, the DLT sector is rated Medium risk overall.



RESULTS OF DATA ANALYSIS

The data analysis exercise was undertaken in order to analyse the SARs submitted by entities within the DLT sector during the years January – December 2018, 2019 and 2020.

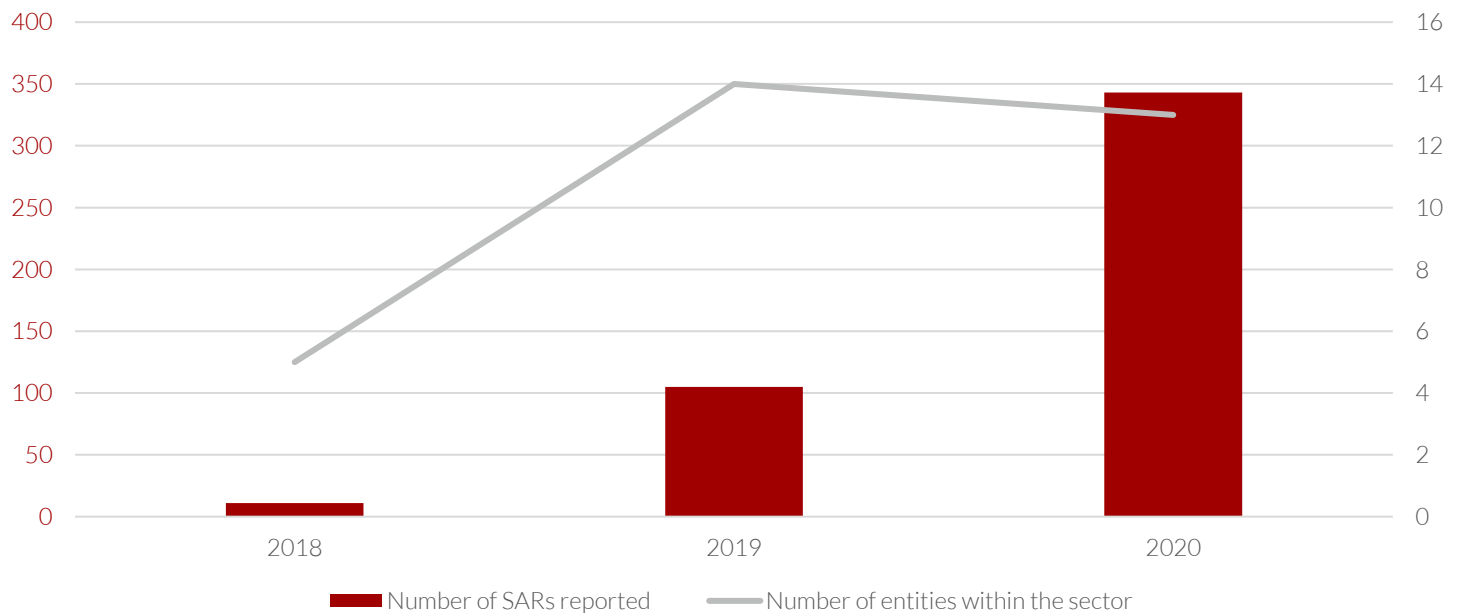
The results have been included below.

Number of regulated DLT firms within the sector

2018	2019	2020
5	14	13

Number of SARs received per regulated DLT firm

DLT entity	2018		2019		2020	
	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported
DLT Entity 1	2	18.18%	-	-	-	-
DLT Entity 2	-	-	-	-	152	44.31%
DLT Entity 3	9	82.82%	67	63.18%	-	-
DLT Entity 4	-	-	32	30.48%	-	-
DLT Entity 5	-	-	5	4.76%	135	39.36%
DLT Entity 6	-	-	1	0.95%	44	12.83%
DLT Entity 7	-	-	-	-	3	0.87%
DLT Entity 8	-	-	-	-	2	0.58%
DLT Entity 9	-	-	-	-	4	1.17%
DLT Entity 10	-	-	-	-	3	0.87%
Total	11	100%	105	100%	343	100%

**Number of SARs reported vs Number of Entities within the Sector**

Although five DLT providers were authorised in 2018, the sector was very much in its infancy stage, with the firms receiving authorisation nearer to the end of the year and with low volumes of business. There are also a number of firms that are authorised but are not considered to be actively trading for various reasons.

The number of SARs raised has substantially increased year on year, generally representing an increase in SARs as the industry grew, but also evidently highly concentrated amongst a small number of DLT firms. In 2019, three firms account for over 95% of SARs reported and in 2020, two firms account for over 83% of SARs reported.

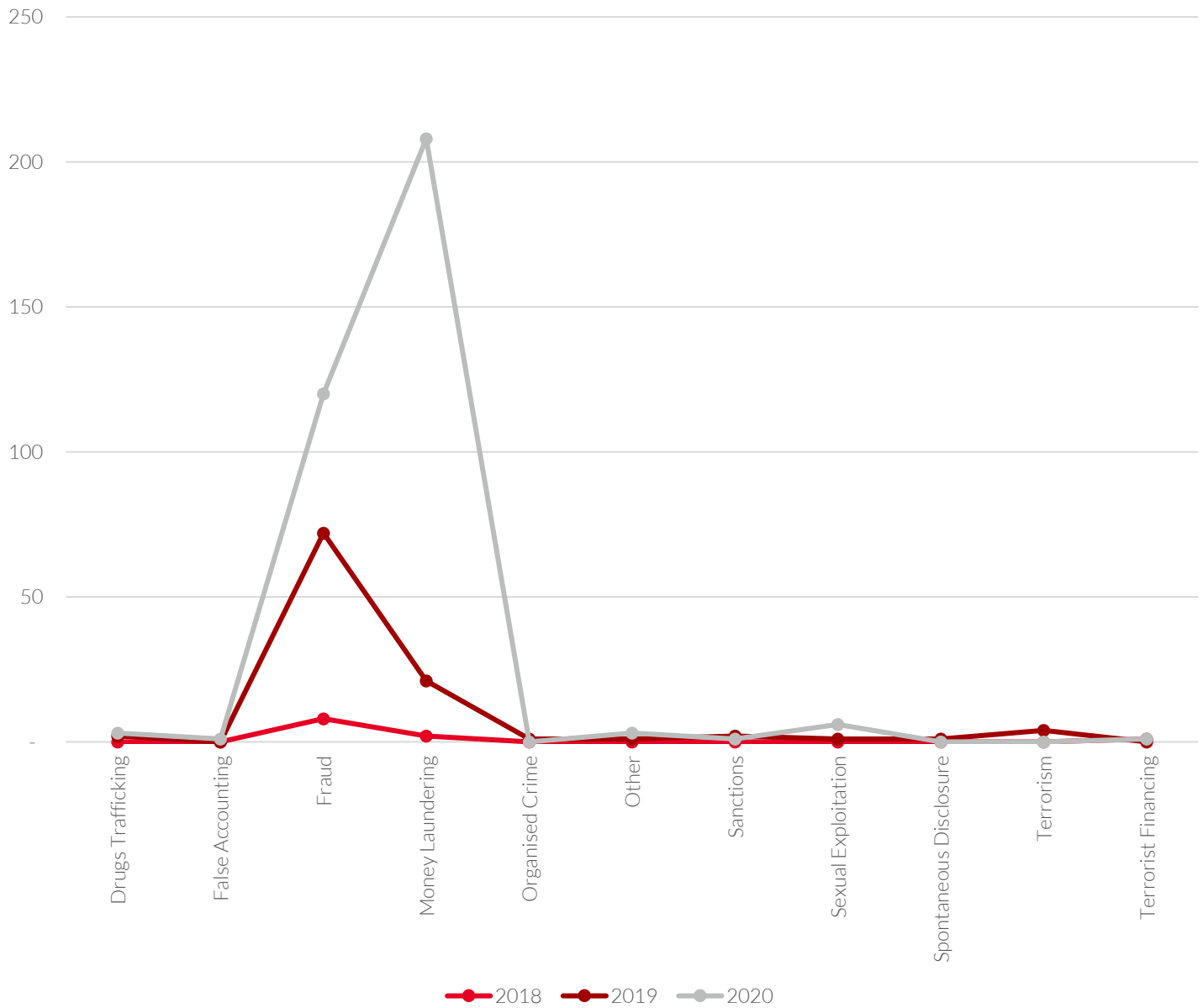
The number of SARs received from the remaining entities are minimal by comparison and raise various questions as to the identification and reporting of potentially suspicious behaviour within the industry.

- Is there a trend for SARs being filed in “defence” by certain DLT entities? For example, is there a generally held view by some MLROs that it is better to report a particular type of SAR, and is this driven by compliance concerns instead of genuine suspicions?
- Is there a prevalence of certain types of potentially suspicious behaviour occurring within the client base of some companies over others?
- Is there a lack of understanding by some firms as to the types of activities that should be reported to the GFIU?

In order to present findings to the above questions, further data analysis was undertaken.



Number of SARs reported by principal suspected criminality



Overwhelmingly, the data above demonstrates that Money Laundering and Fraud are the dominant suspected criminalities reported by MLROs within Gibraltar’s DLT sector and the increase in SARs reported reflect the growth within the sector. There will be SARs where there are multiple suspected criminalities. Themis works on a ‘principal crime system’, which means that in cases which contain more than one type of offence, it will record the principal suspected criminality. As this is a subjective assessment, there may be inconsistencies between MLROs. There are instances where MLROs have more information than what is included within the SAR, which determines what suspected criminality they record. When there are high risks criminalities like Terrorist Financing, Sexual Exploitation, etc. involved, these should always be recorded as the suspected criminality. Within both the Fraud and Money Laundering typologies, there is a spread of suspicious behaviours reported and these have been analysed further below.



GROUNDS FOR SUSPICION

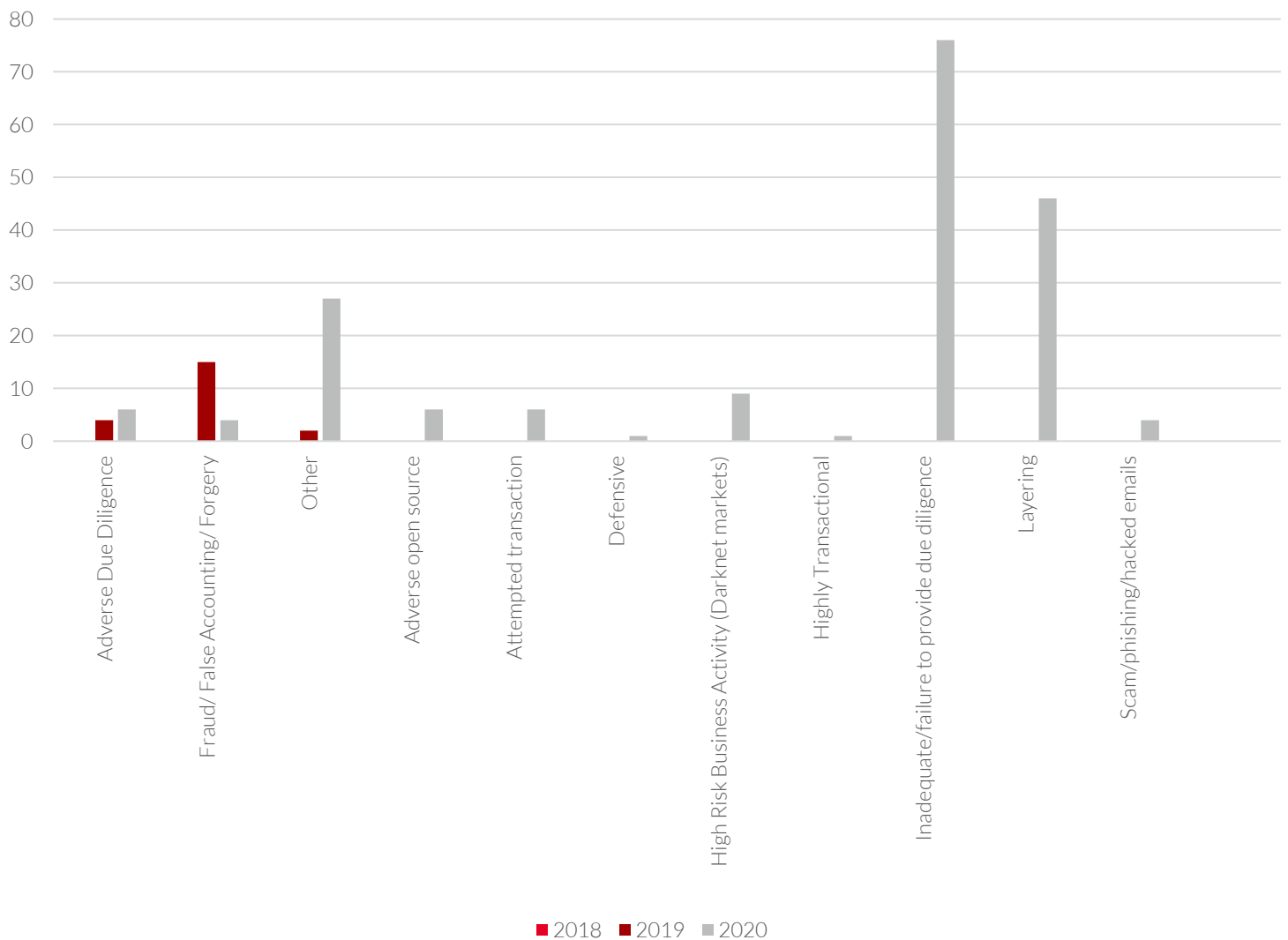
As is the case with suspected criminality, there are SARs which have multiple grounds for suspicion. During the operational analysis of the SAR, the GFIU will record the principal grounds for suspicion. The GFIU’s internal Themis system is designed to select one ‘grounds for suspicion’ category which provides a more comprehensive presentation of statistical data in line with international standards of recording data. However, although some SARs may appear similar, an in depth analysis of each SAR will determine the most appropriate grounds for suspicion to be recorded.

The narrative of the SAR will include all the grounds for suspicion and these are searchable by key words.

As the majority of SARs reported relate to suspected Money Laundering and fraud related offences as detailed above, further data analysis was undertaken to provide insights into the grounds for suspicion that resulted in SAR disclosures.

MONEY LAUNDERING

SARs raised by grounds for suspicion - Money Laundering





In 2019, both the receipt of Adverse Due Diligence and Fraud, False Accounting or Forgery of documentation were reported. In 2020, the provision of inadequate due diligence or the failure to provide due diligence were overwhelmingly reported to the GFIU. Other highly reported suspicions included layering and suspected High Risk Business Activity relating to the darknet. Layering has been reported when illicit fiat funds are converted into Virtual Assets in order to obscure their origins. The reporting of High Risk Business Activities relating to the darknet have also increased and there are well publicised reports of entities on the darknet providing layering services in order to help clients conceal the source or owners of Virtual Assets.

As the reporting of the provision of inadequate due diligence or the failure to provide appropriate due diligence were overwhelmingly reported as Money Laundering related offences, the below will focus on some of the most frequently evidenced reasons for reporting.

As is apparent in the previous chapters on Gaming and E-money, whose sectors also reported this suspected criminality overwhelmingly, the collection of due diligence occurs at different stages within a client relationship. Due diligence is requested at the client onboarding stage, where an individual applies to become a client of the DLT firm and provides initial personal identification details, such as their name, address, date of birth etc. Firms need to identify the client and then verify using a risk based approach. There is some evidence of MLROs raising SARs at this stage before a client has been accepted or funds have been deposited which may partially account for the high number of SARs reported for this suspicion.

A feature of Gibraltar's DLT regulatory regime is the requirement for both transaction monitoring and the prevention, detection and disclosure of financial crime risks, including the verification of valid KYC and other due diligence. The requirement to collect due diligence extends further than the initial client onboarding stages and DLT firms are required to monitor their clients on an ongoing basis.

Many of the SARs arise from a client's use of false identification documents, for example, or inadequate provision of evidence to support the source of funds being used to purchase Virtual Assets.

Number of SARs raised by regulated entity with grounds of suspicion recorded as inadequate/failure to provide due diligence.

During 2018 and 2019 there were two and zero SARs raised respectively, relating to due diligence. In 2020, however, two firms reported due diligence related SARs, with one firm reporting over 96% of the total due diligence related SARs received by the GFIU and 110 due diligence related SARs filed.

The results of this analysis could arise for a number of reasons and these could include:

- The DLT firm reporting the highest number of due diligence related SARs is reporting a number of SARs which could be of little intelligence value or is reporting in a defensive manner to avoid potential regulatory/compliance issues; and/or
- The remaining DLT firms are not identifying potential red flag indicators of suspected Money Laundering relating to due diligence which causes the above DLT firms' reporting to seem too high by comparison.



In order to aid MLROs in understanding the typologies that may present in the DLT industry relating to due diligence failures, the following examples are of importance to note:

- Clients conducting large initial deposits to open a new relationship with a DLT firm which are inconsistent with their client profile (which can include their employment, evidence of source of wealth, age etc.);
- Incomplete or insufficient KYC information provided, or a client declines requests for KYC documentation or ignores inquiries regarding source of funds to support deposits;
- A client has inadequate knowledge or provides inaccurate information about the transaction, the source of funds, or the relationship with the counterparty;
- A client provides forged documents or has edited photographs and/or identification documents as part of the on-boarding process; and
- A client purchases large amounts of Virtual Assets not substantiated by available wealth or consistent with their historical financial profile, which may indicate Money Laundering, a money mule, or a fraud victim.

These examples are not exhaustive but should provide the reader with an understanding of the types of suspicious behaviour that could indicate a need for a SAR to be reported to the GFIU.

LAYERING

During 2018 and 2019, there were no SARs for which layering was the principal grounds for suspicion. In 2020, however, two firms reported layering related SARs, with one firm reporting over 92% of the total layering related SARs received by the GFIU. Similar to the assessment undertaken on due diligence related SARs above.

The results of this analysis could arise for a number of reasons and these could include:

- The DLT firm reporting the highest number of layering related SARs is reporting a number of SARs which could be of little intelligence value or is reporting in a defensive manner to avoid potential regulatory/compliance issues; and/or
- The remaining DLT firms are not identifying potential red flag indicators of suspected Money Laundering relating to layering which causes the above DLT firms' reporting to seem too high by comparison.

In order to aid MLROs in understanding the typologies that may present in the DLT industry relating to layering, the following examples are of importance to note:

- Structuring Virtual Asset transactions in small amounts, or in amounts under record-keeping or reporting thresholds, similar to layering traditional cash transactions;
- Making multiple-high value transactions in short succession, in a staggered or regular pattern, with no further transactions recorded during a long period afterwards;
- The transfer of Virtual Assets immediately to multiple other DLT providers, especially those where the client may not live; and
- Depositing Virtual Assets at an exchange and immediately withdrawing them without additional exchange activity, or converting the Virtual Assets to multiple types of Virtual Assets, incurring additional transaction fees, without logical explanation (such as portfolio diversification).

These examples are not exhaustive but should provide the reader with an understanding of the types of suspicious behaviour that could indicate a need for a SAR to be reported to the GFIU.

**SARs have been reported to the GFIU for suspicions such as:**

- Transfers to and from the darknet to addresses identified as connected to high risk categories;
- Accounts created by clients who are not the typical user of DLT due to their backgrounds. The suspicions are that they are mules or their identities have been used by OCGs;
- Adverse open media linking the client to ponzi schemes and fraud;
- Deposit of various small amount and immediate transfer of the whole amount to another VASP;
- Use of forged identity documents; and
- Value of transactions inconsistent with the known profile of the client.

Defensive SARs

	2018		2019		2020	
GFIU conclusion	Yes	No	Yes	No	Yes	No
Defensive SAR	-	10	18	81	25	318

As described earlier in the chapter, the data analysis undertaken aimed to assess whether there was a culture of defensive SARs submitted to the GFIU by the Gibraltar DLT sector. A defensive SAR arises where an activity or a transaction is deemed not suspicious upon further analysis by the GFIU. SARs are required to be filed when a transaction or an attempted transaction involve funds derived from any illegal activity, or when the transaction has no apparent lawful purpose. As the number of SARs received within the DLT sector have increased significantly over the periods analysed, the analysis above attempts to assess whether the number of defensive SARs raised has also increased. Many entities are wary to be seen by both the GFIU and by their regulator as being complacent or soft on potential instances of Money Laundering. As regulatory and legal scrutiny has increased in this area, so has the risk of regulatory and reputational risk to these entities and so the number of SARs deemed to have been filed in a defensive manner are likely to be explained by this. However, it is important to note that the volume of additional workload created by these defensive SARs where no suspicious activity is contained within have a negative impact on the GFIU, and may even lead to a dilution on the value of SAR reporting as a whole. Whilst the number of defensive SARs are increasing year on year, they are not immediately concerning in this sector when compared to the total SARs deemed to be non-defensive.

Links to Politically Exposed Persons (“PEPs”)

	2018		2019		2020	
GFIU conclusion	Yes	No	Yes	No	Yes	No
Link to PEP	-	11	4	101	2	341

The above analysis suggests that there is very little evidence of SARs raised by DLT entities containing a link to a PEP, which is consistent with both the Gaming, and E-Money sectors analysed previously. This is reported by the MLROs when raising a SAR and both regulations and legal frameworks within Gibraltar require that EDD be applied to all PEPs, including immediate family and known close associates. For any client deemed to be a PEP, specific approval must be obtained for the account opening to continue, the source of funds/wealth must be established and enhanced ongoing monitoring must be applied to the account.



04 Banking Sector





BACKGROUND TO THE SECTOR

Gibraltar hosts 11 banks, which are made up of a mix of retail, commercial and private banks.

The NRA 2020 notes that local banking sector represents the majority of transactions with jurisdictions deemed as posing a higher risk, in terms of amounts of inflows and outflows. However, this is as expected given the key role of credit institutions within the local financial services industry. For the purposes of this analysis, two Banks, which provide E-money and DLT services in have been classified as an E-money firm and a DLT firm respectively and are not included within this chapter.

Whilst there are a small number of Banks, the volume and value of financial transactions generated is substantial with Moneyval noting total banking deposits of GBP 5.9 billion, 76,193 active clients and GBP 10.4 billion in funds under management as at April 2019.

The primary financial crime risk associated with deposit-taking institutions is that perpetrators may place the proceeds of crime into the financial system through the regulated credit and financial sector in order to hide its illegitimate origin. Corporate structures are exposed to Money Laundering as they can be set up in ways that seek to make the identity of the beneficial owner harder to establish particularly when trade based transactions are linked to other jurisdictions with weaker AML/CFT regimes that require less transparency. Cash intensive business poses Money Laundering risks to banks as perpetrators run or use cash based business to commingle illegally obtained funds with cash actually generated legally by the business. The risks linked to forged documentation also affects the level of risk exposure, while the increasing role of intermediaries and facilitators working for organised crime groups can also affect the inherent risk of these products.

Perpetrators have also been known to attempt to disguise and invest the proceeds of crime by way of real-estate investment, with the proceeds used for deposits, repayments and early redemption. The assessment of the Money Laundering threat related to mortgage credit shows that organised crime organisations have frequently used this method. They are well equipped to provide false documentation and the structure of the mortgage (with third-party involvement) helps them to hide the real beneficiary of the funds. Mortgage credit constitutes an easy way to enable criminals to own several properties and to hide the true scale of their assets. This method is still used for the integration phase (mostly for lower amounts, as it does not require sophisticated operations). However, it is more often used in combination with concealment of the beneficial owner of real estate behind a complex chain of ownership.

Wealth management/private banking industry in Gibraltar is small but still presents a ML/TF risk due to the more complex structures that may exist in the arrangements to protect the client's wealth, which may not only include corporate and trust structures but also the use of various intermediaries and advisors. Wealth management and private banking services are judged to be particularly exposed to the risk of being used to launder the proceeds of overseas corruption.

**The NRA 2020 rated the Money Laundering threat of the Banking sector as follows:**

- High Risk for Deposit Taking;
- Medium Low Risk for Corporate Banking;
- Medium Low Risk for Broker Deposits;
- Medium Low Risk for Lending Activities;
- Medium Low Risk for Private Banking/Wealth management; and
- Low Risk for Safe Custody.

RESULTS OF DATA ANALYSIS

The data analysis exercise was undertaken in order to analyse the SARs submitted by entities within the Banking sector during the years January – December 2018, 2019 and 2020.

The results have been included below.

Number of regulated banks within the sector

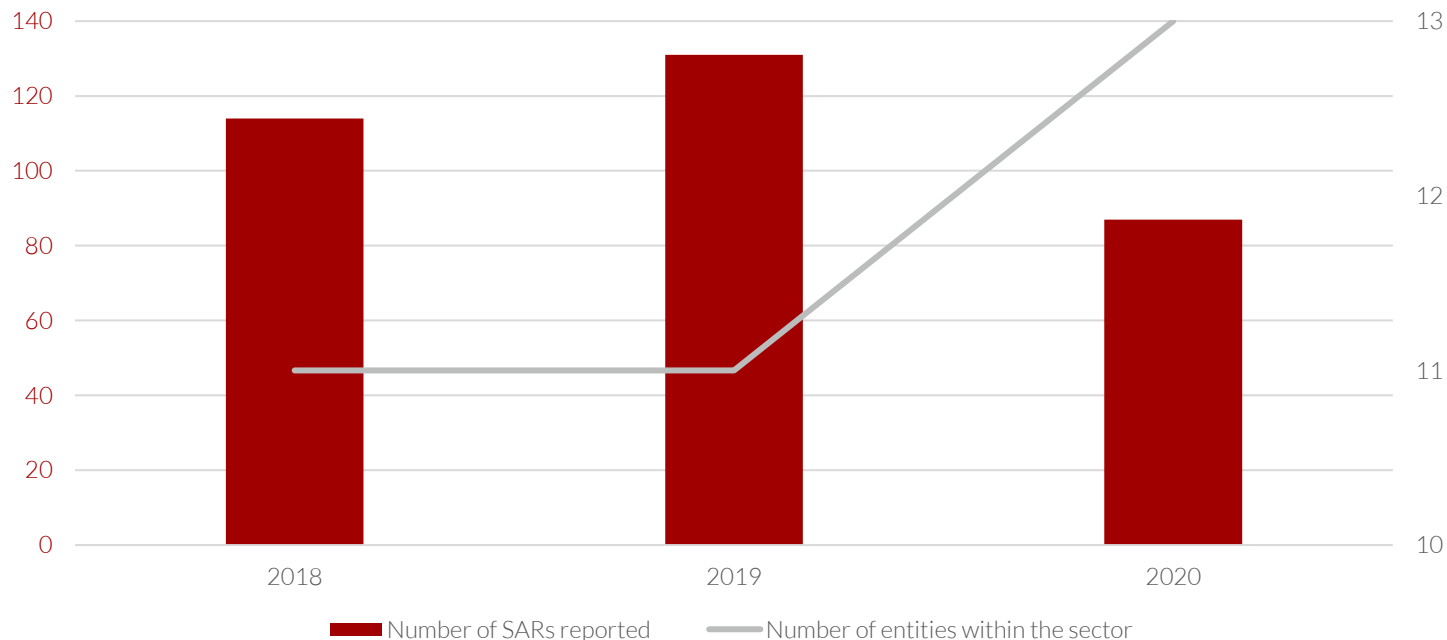
2018	2019	2020
11	11	13

Number of SARs received per bank

Banking entity	2018		2019		2020	
	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported
Banking Entity 1	7	6.14%	26	19.85%	14	16.09%
Banking Entity 2	3	2.63%	1	0.76%	4	4.60%
Banking Entity 3	26	22.81%	59	45.05%	21	24.14%
Banking Entity 4	45	39.47%	6	4.58%	-	-
Banking Entity 5	1	0.88%	4	3.05%	8	9.20%
Banking Entity 6	12	10.53%	9	6.87%	21	24.14%
Banking Entity 7	10	8.77%	8	6.11%	7	8.05%
Banking Entity 8	10	8.77%	18	13.74%	10	11.49%
Banking Entity 9	-	-	-	-	1	1.15%
Total	114	100%	131	100%	87	100%



Number of SARs reported vs Number of Entities within the Sector



The number of SARs reported has remained steady across the periods with the highest reporters generally consistent across the periods. The number of SARs reported are highly concentrated within the reporting of three Banks and the decrease seen between the number of overall SARs reported between 2019 and 2020, pertains to a decrease in the number of SARs reported by one bank in particular. A large number of SARs reported by this bank in 2019 were linked, but were reported by the submission of various SARs.

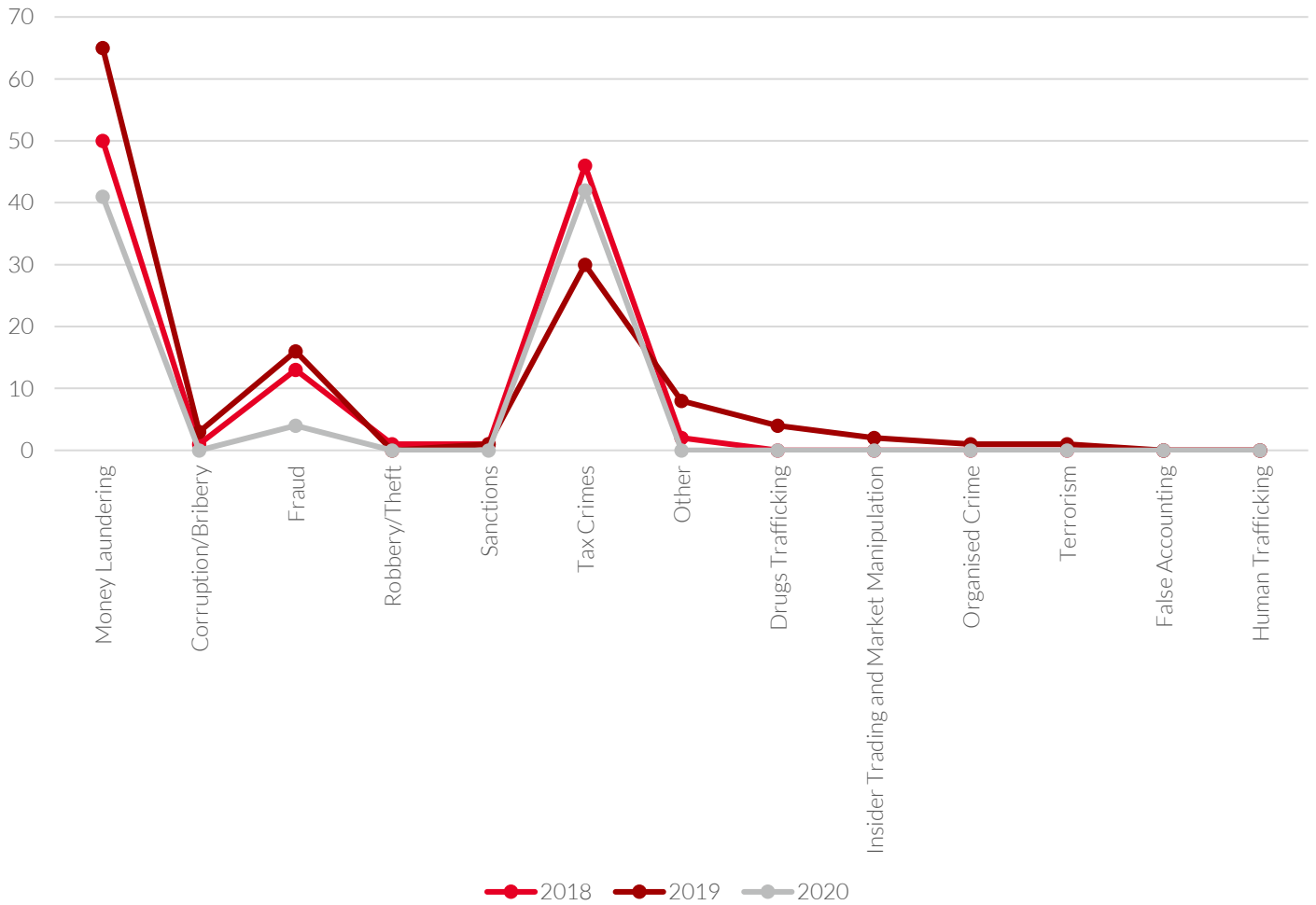
The number of SARs received from the remaining entities are lower by comparison and raise various questions as to the identification and reporting of potentially suspicious behaviour within the industry.

- Is there a trend for SARs being filed in “defence” by certain Banks? For example, is there a generally held view by some MLROs that it is better to report a particular type of SAR, and is this driven by compliance concerns instead of genuine suspicions?
- Is there a prevalence of certain types of potentially suspicious behaviour occurring within the client base of some banks over others?

In order to present findings to the above questions, further data analysis was undertaken.



Number of SARs reported by principal suspected criminality



The data above demonstrates that Money Laundering and Tax Crimes are the dominant suspected criminalities reported by MLROs within Gibraltar’s Banking sector. There will be SARs where there are multiple suspected criminalities. Themis works on a ‘principal crime system’, which means that in cases which contain more than one type of offence, it will record the principal suspected criminality. As this is a subjective assessment, there may be inconsistencies between MLROs. There are instances where MLROs have more information than what is included within the SAR, which determines what suspected criminality they record. When there are high risks criminalities like Terrorist Financing, Sexual Exploitation, etc. involved, these should always be recorded as the suspected criminality. There is a spread of suspicious behaviours reported and these have been analysed further below.



GROUNDS FOR SUSPICION

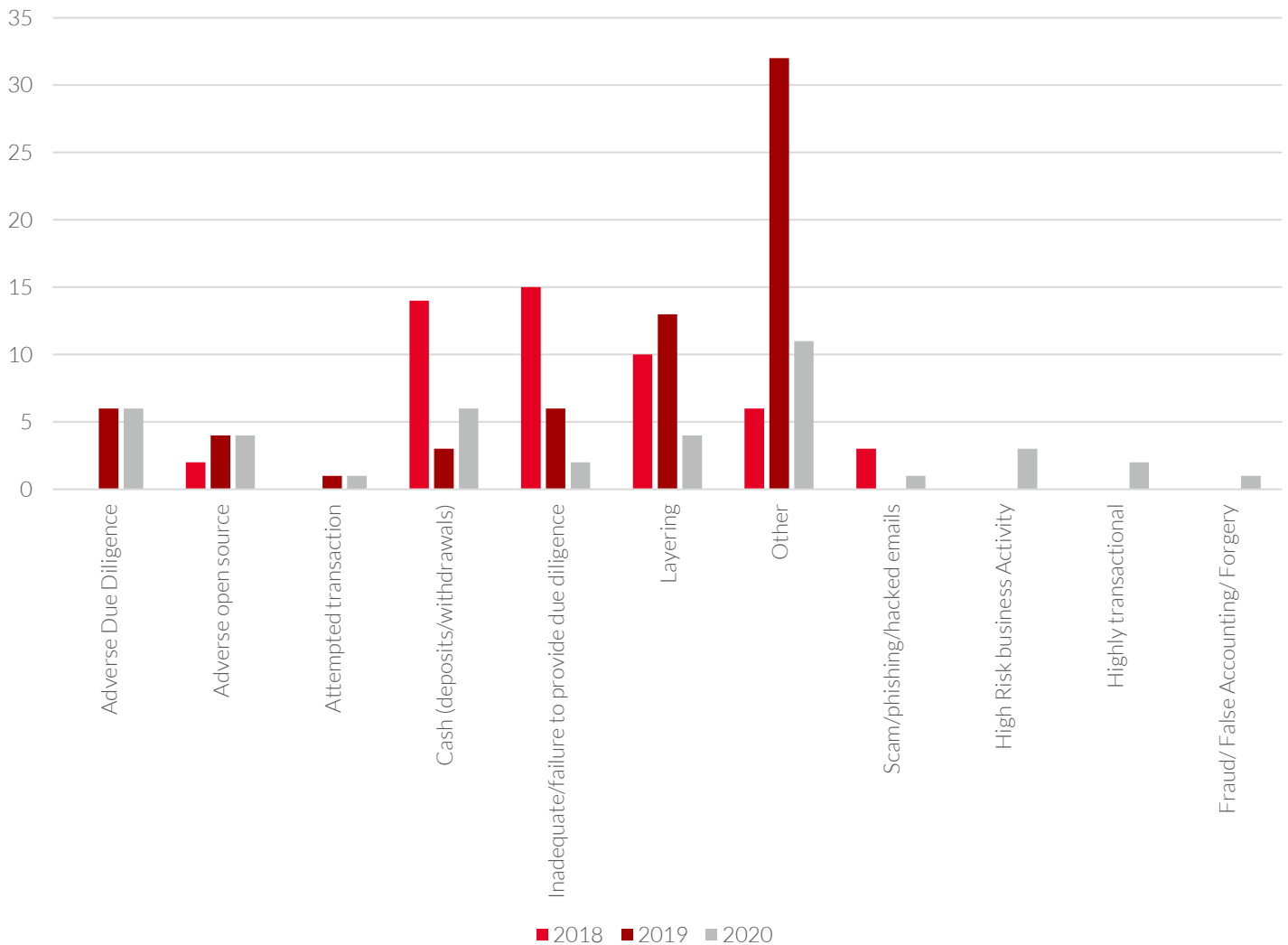
As is the case with suspected criminality, there are SARs which have multiple grounds for suspicion. During the operational analysis of the SAR, the GFIU will record the principal grounds for suspicion. The GFIU’s internal Themis system is designed to select one ‘grounds for suspicion’ category which provides a more comprehensive presentation of statistical data in line with international standards of recording data. However, although some SARs may appear similar, an in depth analysis of each SAR will determine the most appropriate grounds for suspicion to be recorded.

The narrative of the SAR will include all the grounds for suspicion and these are searchable by key words.

As the majority of SARs reported relate to suspected Money Laundering and tax related offences as detailed above, further data analysis was undertaken to provide insights into the grounds for suspicion that resulted in SAR disclosures.

MONEY LAUNDERING

SARs raised by grounds of suspicion - Money Laundering





The majority of SARs raised were filed by MLROs due to perceived inadequate due diligence and/or failure to provide due diligence or source of funds by individual clients. LEA enquiries, adverse opens source, adverse due diligence, unexplained transfers, cash deposits and withdrawals were also reported.

The receipt of due diligence occurs at different stages throughout a client relationship, beginning at the client onboarding stage, where a client applies to become a client of the bank and provides initial personal identification details, such as their name, address, date of birth etc. Firms need to identify the client and then verify using a risk based approach. There is some evidence of MLROs raising SARs at this stage before the banking relationship is onboarded (and any financial flow of funds has been undertaken) which may partially account for the high number of SARs reported for this suspicion.

In order to aid MLROs in understanding the typologies that may present in the banking sector relating to due diligence failures, the following examples are of importance to note:

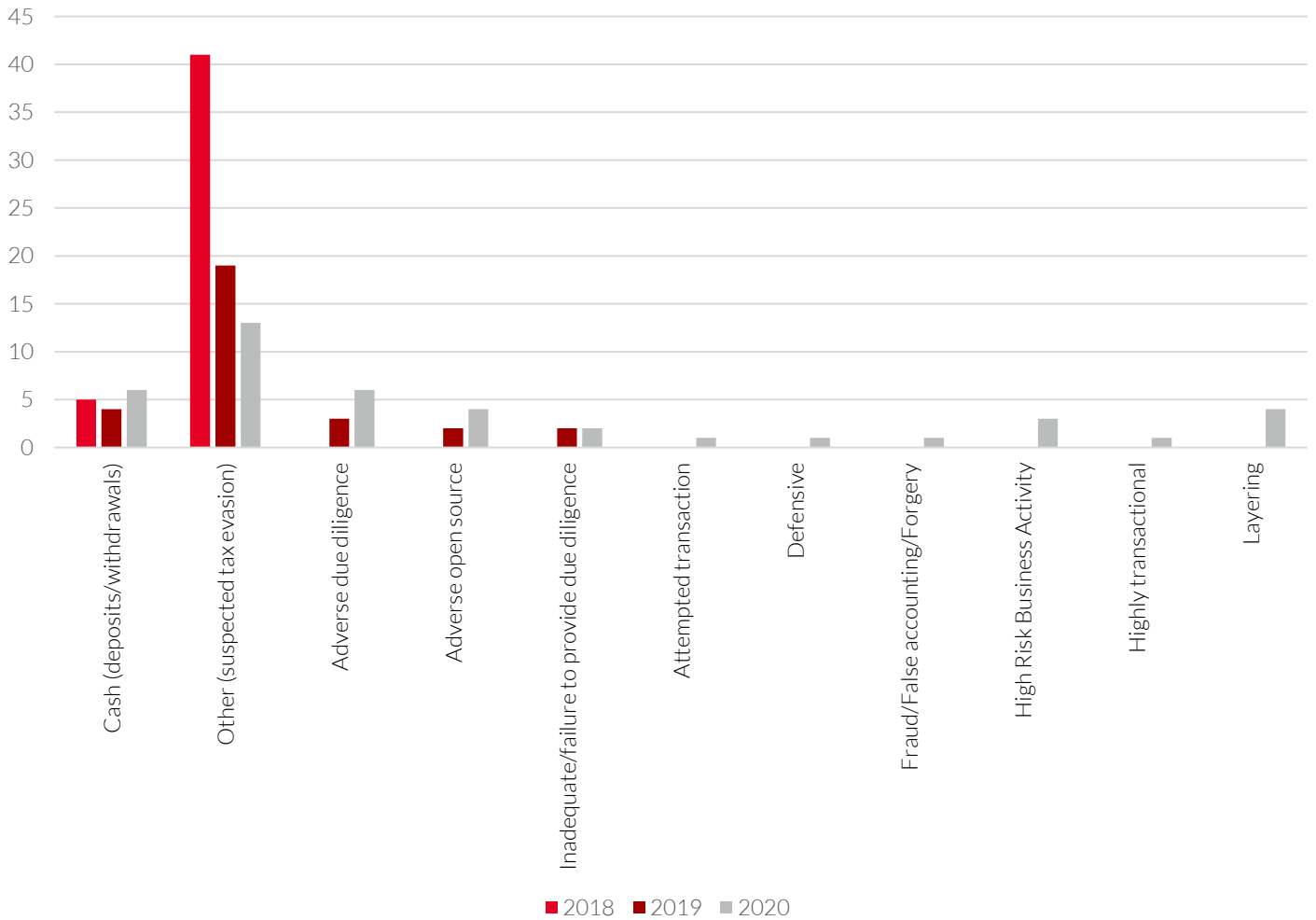
- Potential new clients are reluctant to provide identity details, disclose source of funds or cooperate in any way;
- Inconsistencies in the information provided by clients pertaining to their business or personal activities and source of wealth;
- Clients trying to rush through transactions without providing the requested additional documentation which may be required;
- Clients are unable to explain their source of funds satisfactorily or provide contradictory statements;
- Clients who offer false or fraudulent identification, whether evident from the documents alone, from its lack of connection to the client or from its context in relation to other documents (e.g. use of ID or documents issued in other names without reasonable explanation);
- Clients attempt to obscure the beneficial ownership of assets. Due diligence could be provided for a front company with the aim for this to be used as a legitimate business to hide criminal activity and create legitimate funds;
- Clients who wish to maintain a number of trustees or clients' accounts that do not appear consistent with their type of business;
- Clients provide false/misleading explanations for due diligence purposes;
- Clients become uncontactable when requests for due diligence are made or questions are posed to them;
- Due diligence provided indicates a potential PEP which had not previously been identified;
- Unrealistic turnover or balances detected upon review of company financial statements; and
- Frequent changes to the account address or authorised signatories.

These examples are not exhaustive but should provide the reader with an understanding of the types of suspicious behaviour that could indicate a need for a SAR to be reported to the GFIU.



TAX CRIMES

SARs raised by principal grounds of suspicion - Tax Crimes



In Gibraltar, tax evasion is a predicate offence under the Proceeds of Crime Act (“POCA”). For example, when a client deposits money that should have been paid as taxes due to the tax authorities, that deposit represents the proceeds of crime, as the intention on behalf of the depositor was to evade tax. If a bank knows or suspects that a clients’ funds are the proceeds of crime, it could breach the requirements of POCA if it does not report a SAR and seek consent to hold or process the funds in question.



In order to aid MLROs in understanding the typologies that may present in the banking sector relating to tax evasion, the following examples are of importance to note:

- Client uses an uncommon client structure or overly complex structure without a clear and legitimate commercial purpose or reasonable justification;
- Client has a lack of professional tax advice to support any tax implications of complex structures when questioned;
- Client routinely undertakes transactions involving amounts just below the reporting thresholds (i.e structuring);
- Client undertakes frequently and substantial bank transfers from/to high tax jurisdictions without a legitimate commercial or personal purpose;
- Client fails to disclose dual citizenship or tax domicile;
- Client presents indicators of potential links to another jurisdiction, such as phone numbers in different jurisdictions, place of issue of passport, regular payment patterns etc.; and
- Client shows greater than normal interest in tax related topics or enquires about tax disclosure requirements other than for legitimate tax planning purposes.

These examples are not exhaustive but should provide the reader with an understanding of the types of suspicious behaviour that could indicate a need for a SAR to be reported to the GFIU.

Defensive SARs

	2018		2019		2020	
GFIU conclusion	Yes	No	Yes	No	Yes	No
Defensive SAR	2	112	41	90	8	69

As described earlier in the chapter, the data analysis undertaken aimed to assess whether there was a culture of defensive SARs submitted to the GFIU by the Gibraltar Banking sector. A defensive SAR arises where an activity or a transaction is deemed not suspicious upon further analysis by the GFIU. SARs are required to be filed when a transaction or an attempted transaction involve funds derived from any illegal activity, or when the transaction has no apparent lawful purpose. Many entities are wary to be seen by both the GFIU and by their regulator as being complacent or soft on potential instances of Money Laundering. As regulatory and legal scrutiny has increased in this area, so has the risk of regulatory and reputational risk to these entities and so the number of SARs deemed to have been filed in a defensive manner are likely to be explained by this. Many of the defensive SARs have been because of Law Enforcement Agency (“LEA”) enquiries and adverse open source relating to the client having been arrested. However, it is important to note that the volume of additional workload created by these defensive SARs where no suspicious activity is contained within have a negative impact on the GFIU, and may even lead to a dilution on the value of SAR reporting as a whole.



Links to Politically Exposed Persons (“PEPs”)

	2018		2019		2020	
	Yes	No	Yes	No	Yes	No
GFIU conclusion						
Link to PEP	7	107	3	128	1	86

The above analysis suggests that there is very little evidence of SARs raised by banking entities containing a link to a PEP. As Moneyval and the NRA both noted, the banking sector has the highest volume of transactions with high-risk jurisdictions and so the low number of PEP related SARs in the industry does not necessarily correlate. A PEP relationship is reported by the MLROs when raising a SAR and both regulations and legal frameworks within Gibraltar require that EDD be applied to all PEPs, including immediate family and known close associates. For any client deemed to be a PEP, specific approval must be obtained for the account opening to continue, the source of funds/wealth must be established and enhanced ongoing monitoring must be applied to the account.



Trust and Corporate Services Providers Sector





BACKGROUND TO THE SECTOR

Gibraltar has a large Trust and Corporate Services Provider (“TCSP”) sector and as noted in the NRA, over 98% of all Gibraltar legal entities are managed through TCSPs. TCSPs locally provide company and trust management services. The sector is internationally orientated, focusing mainly on the UK market.

TCSPs form part of groups comprised of companies and individuals that are authorised by the GFSC to act in this capacity. Whilst some TCSPs provide the full range of company management services, other provide reduced services and the level of control and monitoring exercised is dependent on this. A number of TCSPs also provide pension trusteeships.

Some TCSPs or individuals within these also hold licences within other reporting sectors, such as legal firms, accountancy, auditors and investment funds firms. There are reporting entities that have associated businesses that will have submitted a single SAR in respect of multiple sectors. These SARs are recorded according to the principal reporting entity selected by the MLRO.

The Proceeds of Crime Act extends requirements for AML/CFT checks to be undertaken by TCSPs including client due diligence, and the identification of PEPs as well as ongoing transaction monitoring requirements. All TCSPs within Gibraltar are subject to AML/CFT requirements including the mitigation and management of any potential AML/CFT risks.

The NRA 2020 rated the Money Laundering threat of the TCSP sector as follows:

- Medium High Risk for the Creation of Legal Entities and Legal Arrangements;
- Medium Low Risk for Business Activities of Legal Entities and Legal Arrangements;
- Low Risk for the Termination of Legal Entities and Legal Arrangements;
- Medium Low Risk for Private Companies;
- Medium Low Risk for Private Companies;
- Medium Low Risk for Foreign Companies carrying on business in Gibraltar;
- Low Risk for Public Companies;
- Low Risk for Limited Liability Partnerships;
- Medium Low Risk for Trusts; and
- Medium Low Risk for Foundations.

The NRA highlights that as a regional finance centre, Gibraltar would be a likely target where launderers or financiers of terrorism may look to exploit potential weaknesses in the legal or regulatory framework.

RESULTS OF DATA ANALYSIS

The data analysis exercise was undertaken in order to analyse the SARs submitted by entities within the TCSP sector during the years January – December 2018, 2019 and 2020.

The results have been included below.

Number of regulated TCSPs within the sector

2018	2019	2020
58	57	51

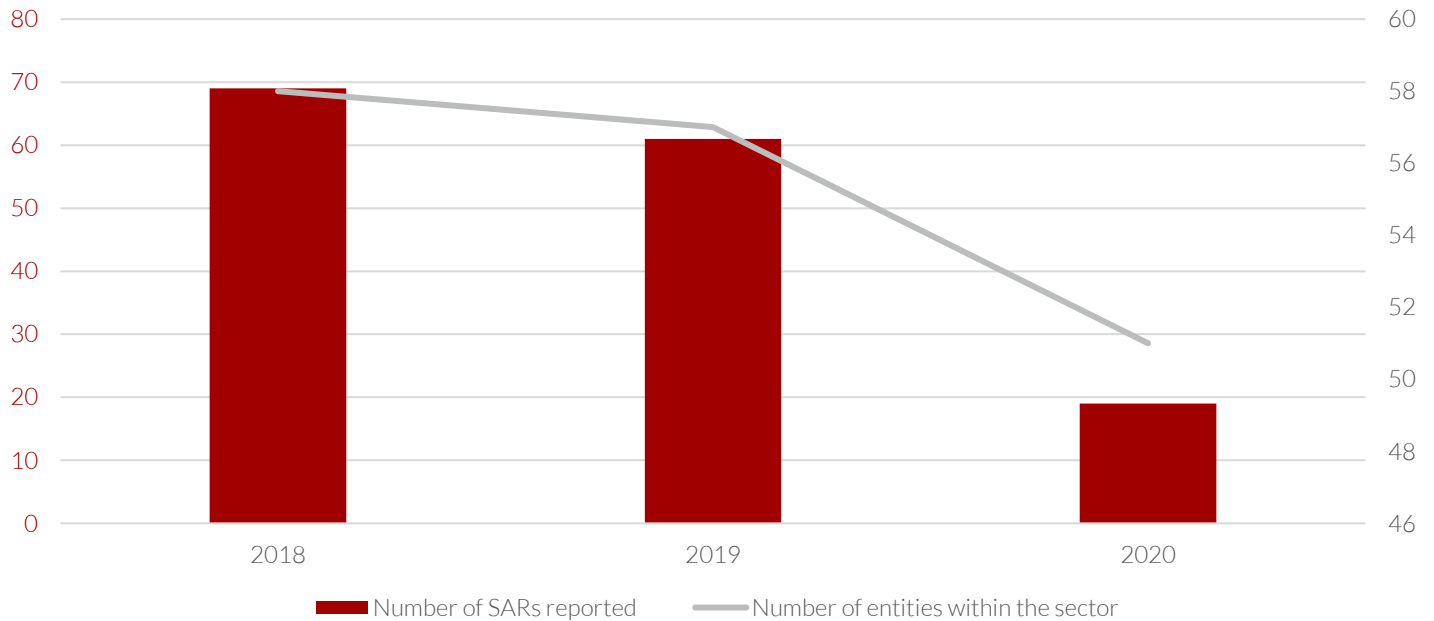


Number of SARs received per regulated TCSP

TCSP	2018		2019		2020	
	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported
TCSP Entity 1	2	2.90%	1	1.64%	-	-
TCSP Entity 2	1	1.45%	1	1.64%	-	-
TCSP Entity 3	1	1.45%	1	1.64%	-	-
TCSP Entity 4	2	2.90%	3	4.92%	-	-
TCSP Entity 5	1	1.45%	-	-	1	4.76%
TCSP Entity 6	5	7.25%	3	4.92%	1	4.76%
TCSP Entity 7	1	1.45%	-	-	-	-
TCSP Entity 8	6	8.70%	1	1.64%	-	-
TCSP Entity 9	1	1.45%	4	6.56%	1	4.76%
TCSP Entity 10	3	4.35%	1	1.64%	-	-
TCSP Entity 11	5	7.25%	7	11.48%	-	-
TCSP Entity 12	1	1.45%	-	-	-	-
TCSP Entity 13	3	4.35%	-	-	-	-
TCSP Entity 14	3	4.35%	-	-	-	-
TCSP Entity 15	2	2.90%	1	1.64%	-	-
TCSP Entity 16	7	10.14%	5	8.20%	5	23.81%
TCSP Entity 17	7	10.14%	3	4.92%	4	19.05%
TCSP Entity 18	7	10.14%	9	14.75%	1	4.76%
TCSP Entity 19	5	7.25%	4	6.56%	-	-
TCSP Entity 20	1	1.45%	-	-	-	-
TCSP Entity 21	4	5.80%	-	-	1	4.76%
TCSP Entity 22	-	-	6	9.84%	1	4.76%
TCSP Entity 23	-	-	5	8.20%	1	4.76%
TCSP Entity 24	-	-	3	4.92%	-	-
TCSP Entity 25	-	-	1	1.64%	1	4.76%
TCSP Entity 26	-	-	1	1.64%	-	-
TCSP Entity 27	-	-	1	1.64%	-	-
TCSP Entity 28	1	-	-	-	1	4.76%
TCSP Entity 29	-	-	-	-	1	9.52%
Total	69	100%	61	100%	19	100%



Number of SARs reported vs Number of Entities within the Sector



The number of SARs reported remained steady across 2018 and 2019, with a dramatic decrease in 2020. The highest reporters generally reported similar levels of SARs across the three periods. As noted, the number of SARs overall reported within the sector is low when considering that, 98% of all legal entities in Gibraltar are managed by TCSPs and that TCSPs also manage legal entities outside Gibraltar.

Whilst previously MLROs would be providing updates to SARs or submitting consent requests by submitting a new SAR, the Themis functionality to provide updates to existing SARs has been better utilised.

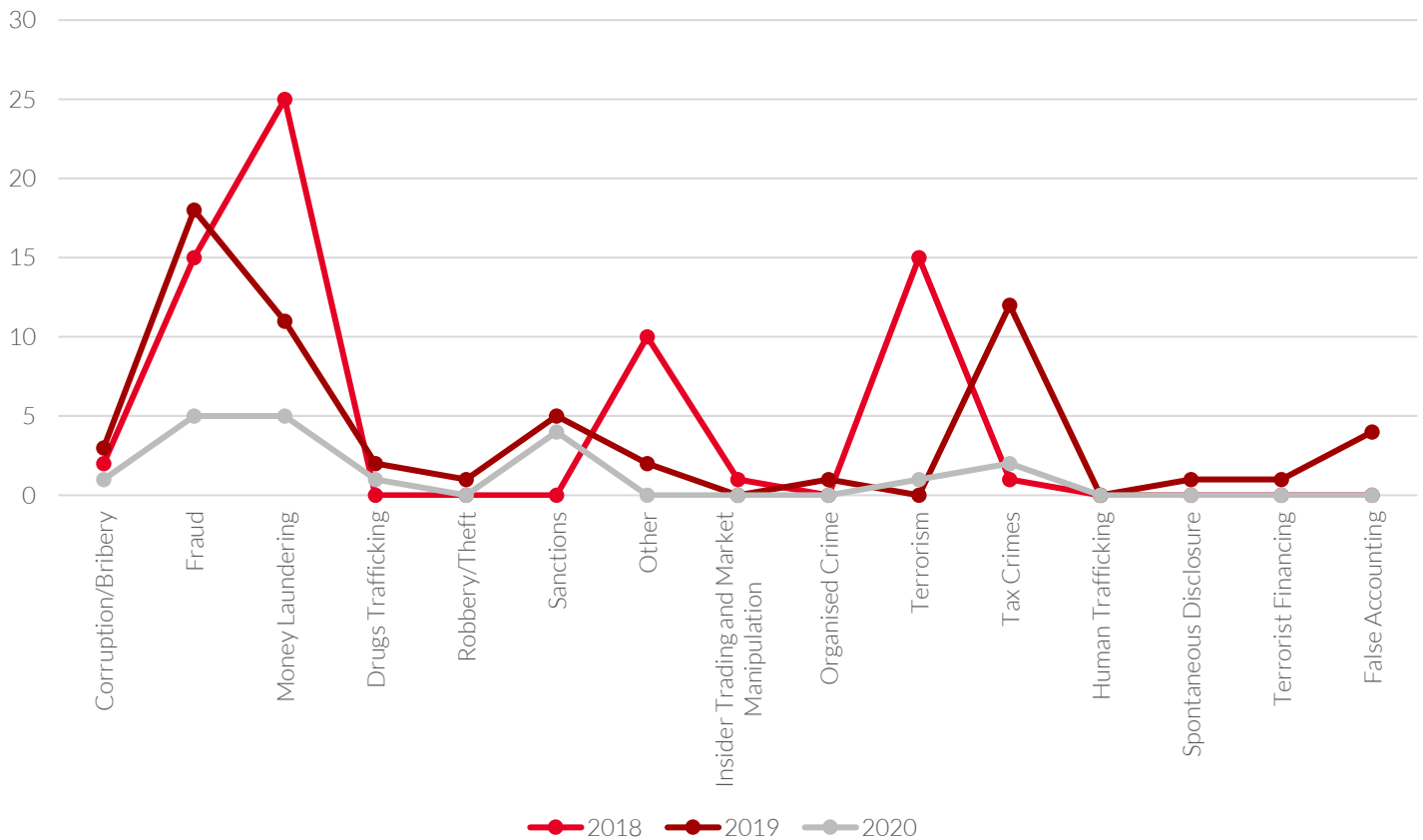
The number of SARs received from the remaining entities are minimal by comparison and raise various questions as to the identification and reporting of potentially suspicious behaviour within the industry.

- Is there a trend for SARs being filed in “defence” by certain TCSPs? For example, is there a generally held view by some MLROs that it is better to report a particular type of SAR, and is this driven by compliance concerns instead of genuine suspicions?
- Are MLROs submitting SARs in respect of all internal suspicions raised or are they analysing and discarding some as not requiring submission?
- Is there a prevalence of certain types of potentially suspicious behaviour occurring within the client base of some companies over others?
- Is there a failure by certain TCSPs to identify and/or report suspicious activities?
- Is there a trend in relation to TCSPs, which rely predominantly on business introduced by third party introducers and intermediaries?
- Are some TCSPs or TCSP services more susceptible to being used for criminal activity?
- Is there a lack of understanding by some firms as to the types of activities that should be reported to the GFU?

In order to present findings to some of the above questions, further data analysis was undertaken.



Number of SARs reported by principal suspected criminality



The data above demonstrates that Fraud, Money Laundering and Tax Crimes are the dominant principal suspected criminalities reported by MLROs within Gibraltar’s TCSP sector. There will be SARs where there are multiple suspected criminalities. Themis works on a ‘principal crime system’, which means that in cases which contain more than one type of offence, it will record the principal suspected criminality. As this is a subjective assessment, there may be inconsistencies between MLROs. There are instances where MLROs have more information than what is included within the SAR, which determines what suspected criminality they record. When there are high risks criminalities like Terrorist Financing, Sexual Exploitation etc. involved these should always be recorded as the suspected criminality. There is a spread of suspicious behaviours reported and these have been analysed further below.

GROUNDS FOR SUSPICION

As is the case with suspected criminality, there are SARs which have multiple grounds for suspicion. During the operational analysis of the SAR, the GFIU will record the principal grounds for suspicion. The GFIU’s internal Themis system is designed to select one ‘grounds for suspicion’ category which provides a more comprehensive presentation of statistical data in line with international standards of recording data. However, although some SARs may appear similar, an in depth analysis of each SAR will determine the most appropriate grounds for suspicion to be recorded.

The narrative of the SAR will include all the grounds for suspicion and these are searchable by key words.

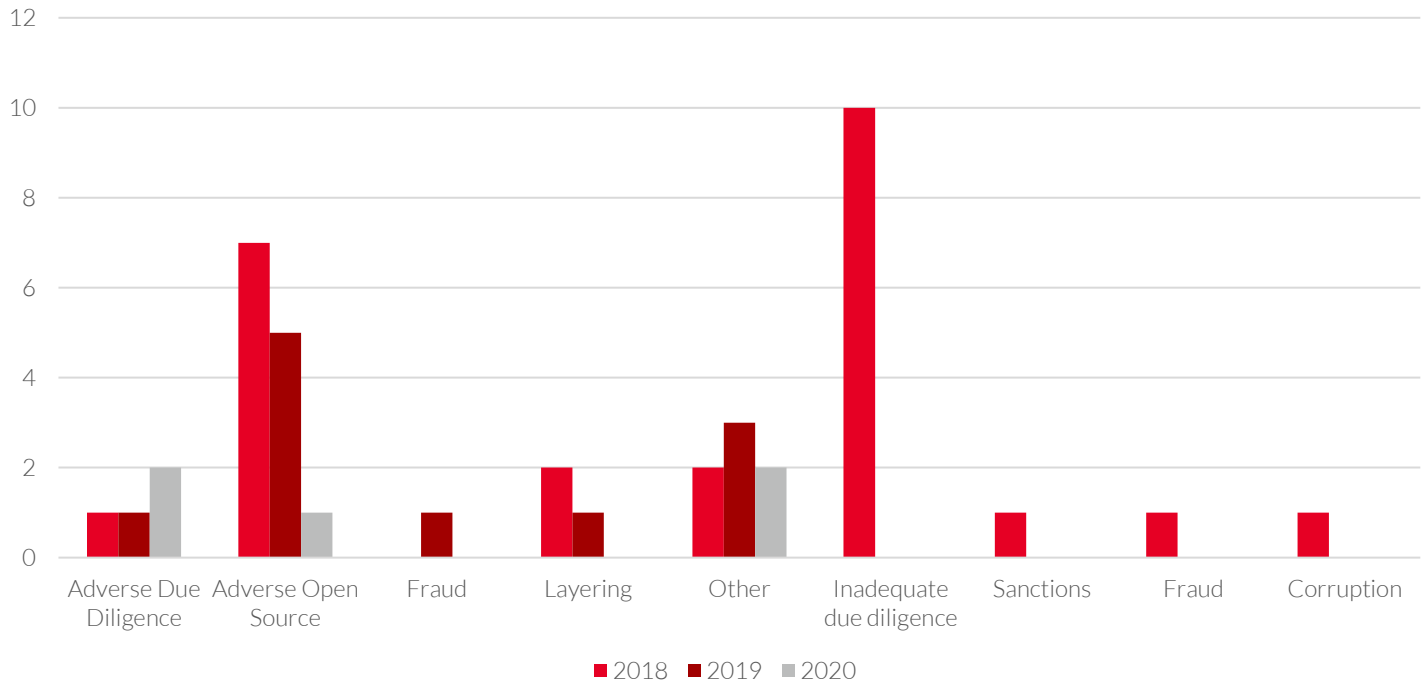
As the majority of SARs reported relate to suspected Money Laundering, fraud and tax crimes related offences as detailed above, further data analysis was undertaken to provide insights into the grounds for suspicion that resulted in SAR disclosures.



MONEY LAUNDERING

During 2018, the highest reported SARs related to TCSPs obtaining inadequate due diligence on clients, which resulted in a suspicion. In 2019 and 2020, adverse due diligence or adverse open source information were the most highly reported grounds for suspicion.

SARs raised by principal grounds for suspicion - Money Laundering



As the reporting of adverse open source information and the provision of inadequate or failure to provide due diligence ranked the highest across all three years, the below will focus on some of the most frequently evidenced reasons for reporting.

Number of SARs raised by regulated entity with grounds of suspicion recorded as adverse open source information.

During the periods analysed, adverse open source information was reported highly as the reason TCSPs report a SAR. Depending on the services provided TCSPs may not routinely deal directly with a client’s funds, but will be able to focus on the persons they are transacting with and the nature of the services provided. In view of the risks involved, TCSPs must be vigilant at all times and report any suspicious activity where necessary and open source checks provide a useful way of gathering information on clients as part of wider transaction monitoring requirements, and also at the client onboarding stage.



Open source information is information considered widely available, be that via internet searches, social media, the wider online media, the electoral register, sanctions lists, etc. This information is often used to compliment or verify due diligence documentation received and provides the TCSP with further information into a clients' identity, source of wealth etc. When these reviews are performed, any information which is deemed to be adverse or negative is used to assist the TCSP in forming a view on the client and whether or not to proceed with the business relationship, or onboard them in the first place. A significant number of SARs submitted by one of the main reporting TCSP relate to the client companies undertaking activities different to what the reporting firm believed to be the companies' activities. This was mainly identified by open source checks including the firm's website and receipt of correspondence for the client company. This particular firm had a high reliance on the use of intermediaries.

In order to aid MLROs in understanding the typologies that may present in the TCSP sector relating to adverse open source information, the following examples are of importance to note:

- Searches on a client or associate show, for example, adverse media attention, disqualification as a director, convictions for dishonesty or association with bribery in relation to contract procurement;
- Searches indicate connections to politically exposed persons or their family members which were not disclosed;
- Where the client is, or appears to be, acting on behalf of another person, an unwillingness to give the names of the persons they represent;
- The person acting as a director or representative does not appear to be a suitable representative or does not appear to have the expertise that the role requires;
- Frequent changes in ownership, officers, beneficiaries or trustees in an attempt to evade detection of any potential adverse information available;
- Customer unwilling or refusing to provide information including documentary proof of himself or the beneficial owners of trusts or companies;
- Customer carries out transactions for themselves or on behalf of the company that does not correspond with their background;
- The beneficial ownership is veiled in complexity making it impossible to determine;
- The client is secretive about the reasons for the way a company structure is being set up;
- The client's main business rationale is to engage with jurisdictions with, for example, weak anti Money Laundering laws or controls, limited corporate registration requirements, where there is no requirement to update ownership changes, limited beneficial ownership information requirements; and
- The client favours legal entities that are not transparent.

These examples are not exhaustive but should provide the reader with an understanding of the types of suspicious behaviour relating to adverse open source information that could indicate a need for a SAR to be reported to the GFIU.

**Number of SARs raised by regulated entity with principle grounds of suspicion recorded as inadequate due diligence or failure to provide due diligence.**

During 2018, there were 10 SARs reported relating to due diligence which were classified as Money Laundering related. However, the number of SARs generally submitted by the TCSP sector is low relative to the size of the sector.

In order to aid MLROs in understanding the typologies that may present in the TCSP sector relating to due diligence failures, the following examples are of importance to note:

- Potential new clients are reluctant to provide identity details, disclose source of funds or cooperate in any way;
- Inconsistencies in the information provided by clients pertaining to their business or personal activities and source of wealth;
- Clients trying to rush through transactions without providing the requested additional documentation which may be required;
- Clients are unable to explain their source of funds satisfactorily or provide contradictory statements;
- Clients who offer false or fraudulent identification, whether evident from the documents alone, from its lack of connection to the client or from its context in relation to other documents (e.g. use of ID or documents issued in other names without reasonable explanation);
- Clients attempt to obscure the beneficial ownership of assets. Due diligence could be provided for a front company with the aim for this to be used as a legitimate business to hide criminal activity and create legitimate funds;
- Clients who wish to maintain a number of trustees or clients' accounts that do not appear consistent with their type of business;
- Clients provide false/misleading explanations for due diligence purposes;
- Clients become uncontactable when requests for due diligence are made or questions are posed to them;
- Due diligence provided indicates a potential PEP which had not previously been identified;
- Unrealistic turnover or balances detected upon review of company financial statements, that is not in line with the information held by the TCSP on the activity of the client; and
- Frequent changes to the account address or authorised signatories.

These examples are not exhaustive but should provide the reader with an understanding of the types of suspicious behaviour that could indicate a need for a SAR to be reported to the GFIU.

**Defensive SARs**

	2018		2019		2020	
	Yes	No	Yes	No	Yes	No
GFIU conclusion						
Defensive SAR	1	68	11	50	3	16

The data analysis undertaken aimed to assess whether there was a culture of defensive SARs submitted to the GFIU by the TCSP sector. A defensive SAR arises where an activity or a transaction is deemed not suspicious upon further analysis by the GFIU. SARs are required to be filed when a transaction or an attempted transaction involve funds derived from any illegal activity, or when the transaction has no apparent lawful purpose. As the number of SARs received within the TCSP sector have remained relatively stable over the periods analysed, the analysis above attempts to assess whether the number of defensive SARs raised has increased over time. Many entities are wary to be seen by both the GFIU and by their regulator as being complacent or soft on potential instances of Money Laundering. As regulatory and legal scrutiny has increased in this area, so has the risk of regulatory and reputational risk to these entities and so the number of SARs deemed to have been filed in a defensive manner generally can be explained by this. During 2019, there was an increase in the number of defensive SARs reported representing approximately 18% of total SARs. However, the numbers remain relatively low in comparison to the total volume of SARs across other periods.

Links to Politically Exposed Persons (“PEPs”)

	2018		2019		2020	
	Yes	No	Yes	No	Yes	No
GFIU conclusion						
Link to PEP	1	68	5	56	2	17

The above analysis suggests that there is very little evidence of SARs raised by TCSPs containing a link to a PEP, which is consistent with the other sectors analysed previously. This is reported by the MLROs when raising a SAR and both regulations and legal frameworks within Gibraltar require that EDD be applied to all PEPs, including immediate family and known close associates. For any client deemed to be a PEP, specific approval must be obtained for the account opening to continue, the source of funds/wealth must be established and enhanced ongoing monitoring must be applied to the account.



Insurance Sector





BACKGROUND TO THE SECTOR

The insurance sector in Gibraltar is composed primarily of general insurance companies, with a small number of companies underwriting life insurance. The majority of general insurance firms underwrite wholly non-local risks in classes 3 and 10 (motor business) into the United Kingdom. Gibraltar's insurance industry is estimated to underwrite approximately 30% of all UK car insurance policies (its main market).

Non-life insurance policies are generally short-term in nature and serve to provide protection against unexpected loss, such as damage to property. Based on the gross written premiums, the most dominant lines of non-life insurance business are those linked to motor vehicle liability, fire and other forms of damage to property, as well as medical expenses. As detailed above, however, Gibraltar's General Insurance market is predominantly composed of motor vehicle liability. Gibraltar's largest motor insurers are household names in the UK but there are also medium sized and smaller insurers that operate in niche areas of the market offering choice and competition to UK consumers.

Life assurance companies offer a range of investment products, with or without guarantees, and include life insurance benefit as a component. The Gibraltar sector specifically deals mainly with low value policies issued to low risk jurisdictions, with an average value of approximately £3,000.

Insurance managers are authorised to provide managerial functions to licensed Gibraltar insurance or reinsurance companies and/or to give advice. The functions of an insurance manager are similar to the functions of the staff and executive management team of an insurance company. There are also a number of insurance intermediaries based in Gibraltar authorised to sell general insurance and/or life assurance investment products.

Whilst the sector represents one of the most actively used types of financial services in Gibraltar, the sector is one of the lowest SAR contributors over the periods analysed and the predominant predicate offence indicated in these SARs are "fraud" and "Money Laundering".

The NRA 2020 rated the Money Laundering and terrorist financing threats arising from the insurance sector as low risk. The risks of these activities occurring in Gibraltar are mitigated primarily through the legislative requirements and supervisory regimes. The majority of general insurers in Gibraltar are also managed and administered by licenced insurance managers. These firms provide an additional layer of oversight and assessment over the controls employed by the insurance company as well as providing day-to-day management and administrative support. The small number of authorised life assurance firms in Gibraltar, coupled with low premium levels and exposure associated with these firms lessens the potential risk that they pose to the jurisdiction.



RESULTS OF DATA ANALYSIS

The data analysis exercise was undertaken in order to analyse the SARs submitted by entities within the insurance sector during the years January – December 2018, 2019 and 2020.

The results have been included below.

Number of regulated insurance companies, insurance managers and insurance distribution firms within the sector

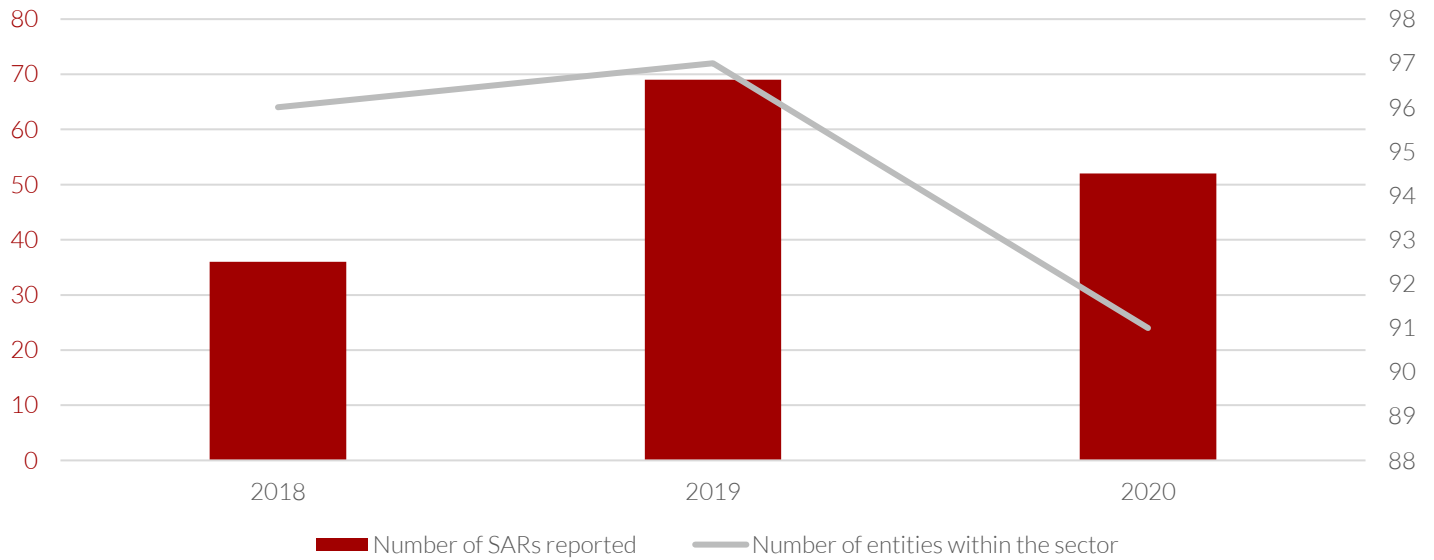
	2018	2019	2020
Insurance Intermediaries	28	29	28
Insurance Companies	63	62	58
Insurance Managers	5	6	5
Total regulated insurance firms	96	97	91

Number of SARs received per regulated insurance company

Insurance entity	2018		2019		2020	
	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported
Insurance Entity 1	7	19.44%	-	-	-	-
Insurance Entity 2	1	2.78%	1	1.45%	-	-
Insurance Entity 3	24	66.67%	1	1.45%	-	-
Insurance Entity 4	1	2.78%	-	-	-	-
Insurance Entity 5	2	5.56%	-	-	-	-
Insurance Entity 6	1	2.78%	-	-	-	-
Insurance Entity 7	-	-	59	85.51%	50	96.00%
Insurance Entity 8	-	-	5	7.25%	-	-
Insurance Entity 9	-	-	2	2.90%	-	-
Insurance Entity 10	-	-	1	1.45%	-	-
Insurance Entity 11	-	-	-	-	2	4.00%
Total	36	100%	69	100%	52	100%



Number of SARs reported vs Number of Entities within the Sector



The number of SARs raised substantially increased in 2019, directly attributable to the number of SARs raised by a single firm. Since 2019, a single firm represented over 85% of SARs. These SARs are also dual disclosed to the UK authorities. Other than the SARs raised by this firm the number of SARs across the sector has seen a significant decline year on year. In 2018, a single firm accounted for 67% of SARs but is no longer reporting.

The number of SARs received from the remaining entities are minimal by comparison and with the sector remaining stable throughout the period under review, the trend raises various questions as to the identification and reporting of potentially suspicious behaviour within the industry.

- Do insurance companies report a lower number of SARs compared to insurance intermediaries and insurance manager?
- Is the sector aware of its Gibraltar reporting obligations?
- Are the fluctuations in SARs reported driven by the nature of suspected criminality, reflecting the changing environment within the sector or are other factors such as 'defensive' reporting influencing the number of SARs reported?
- Is there a prevalence of certain types of potentially suspicious behaviour occurring within the client base of some companies over others?

In order to present findings to the above questions, further data analysis was undertaken.



Number of SARs reported by class of insurance firm

	2018		2019		2020	
	Number of SARs	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported
Insurance Intermediaries	7	19.44%	59	85.51%	50	96.00%
Insurance Companies	26	72.22%	7	10.14%	2	4.00%
Insurance Managers	3	8.33%	3	4.35%	-	0.00%
Total	36	100%	69	100%	52	100%

Insurance is sold through a variety of distribution channels. A significant proportion of insurance policies are sold through intermediaries where the insurer will have limited or no direct contact with the policyholder. In a number of cases, the intermediaries have the initial interaction with the client. Insurance policies are also sold online, where there may not be any face-to-face interaction with the client by the insurer or intermediary. Furthermore, the majority of insurers' clients are based overseas and a number of life insurers outsource AML activities to third parties. This adds to the reliance on intermediaries and outsourced partners to obtain and maintain adequate client due diligence, however the insurer retains full responsibility for AML/CFT processes and controls in such arrangements.

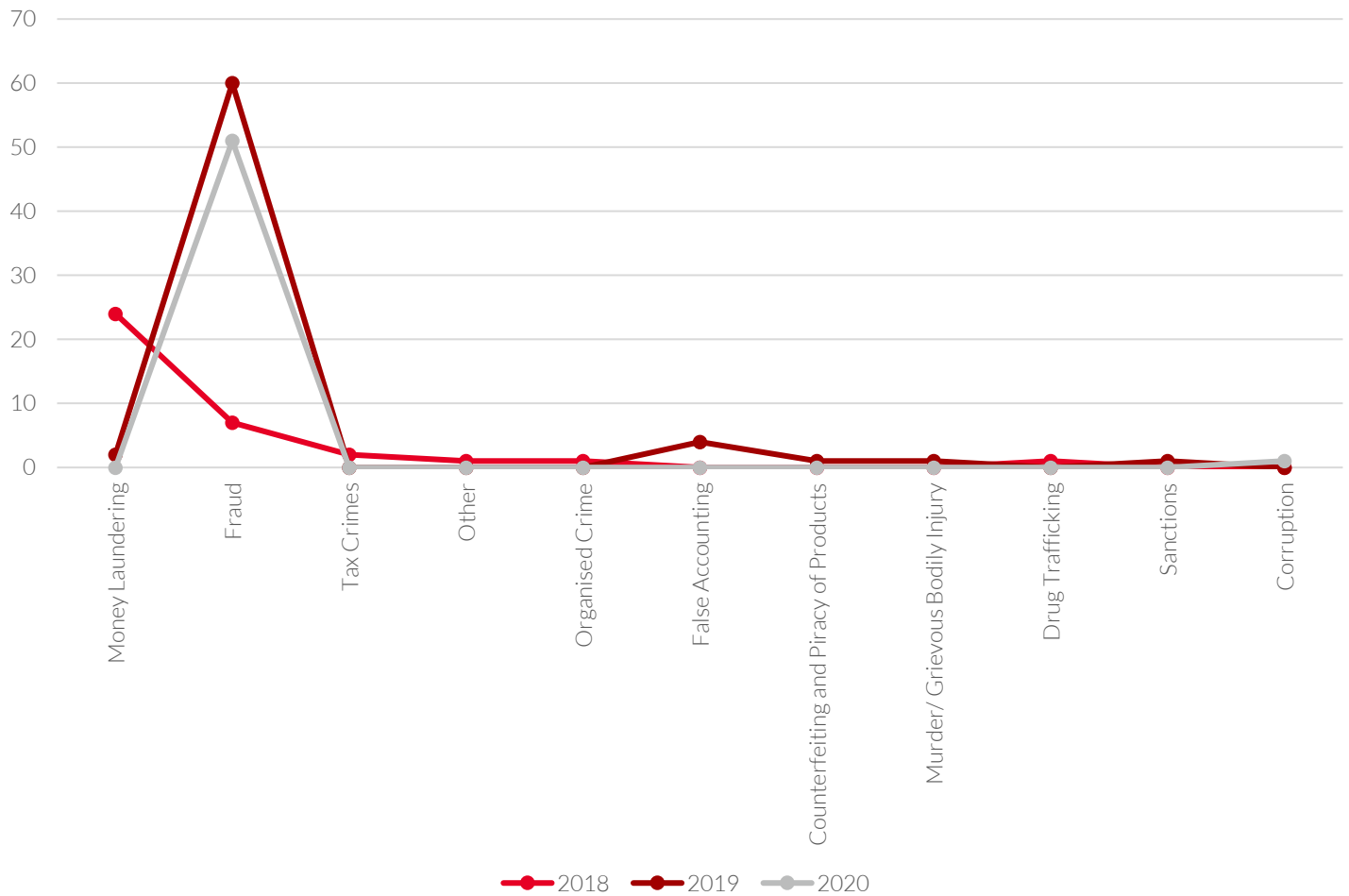
Based on the analysis above, Insurance Intermediaries and Insurance Companies overwhelmingly account for the majority of SARs reported; these results however are skewed given that they represent over 94% of regulated insurance firms each year. The table below highlights the percentage of regulated firms who reported at least one SAR in each period, better representing the distribution of reporting.

Percentage of insurance firms who reported at least one SAR

	2018	2019	2020
Insurance Intermediaries	4%	3%	4%
Insurance Companies	5%	5%	2%
Insurance Managers	40%	33%	-



Number of SARs reported by principal suspected criminality



Overwhelmingly, the data above demonstrates that Money Laundering and Fraud are the dominant principal suspected criminalities reported by MLROs within Gibraltar's Insurance sector. Across both the Fraud and Money Laundering typologies, there is a spread of suspicious behaviours reported and these have been analysed further below, highlighting the significant decrease in the number of Money Laundering SARs..

GROUNDINGS FOR SUSPICION

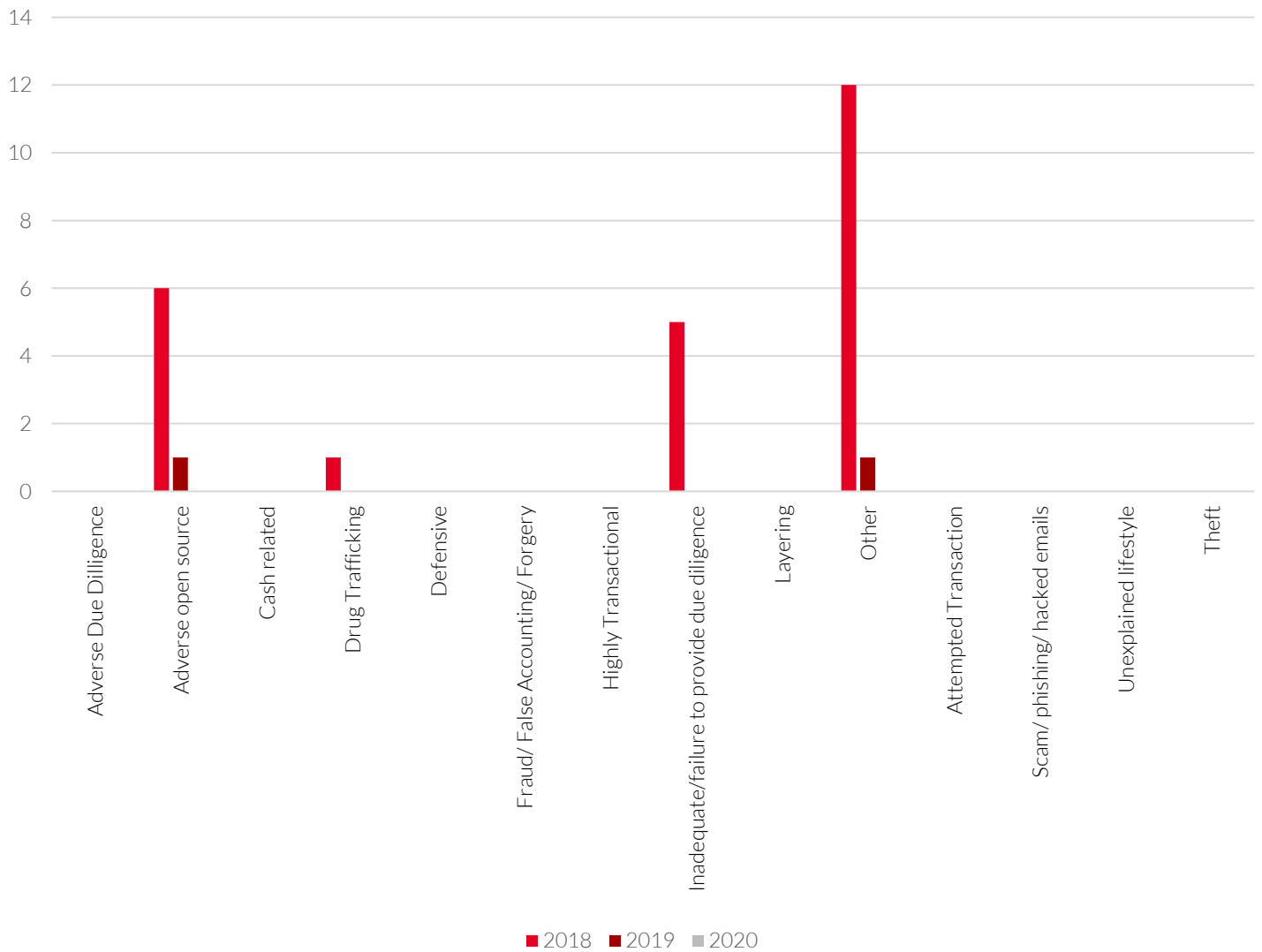
As is the case with suspected criminality, there are SARs which have multiple grounds for suspicion. During the operational analysis of the SAR, the GFIU will record the principal grounds for suspicion. The GFIU's internal Themis system is designed to select one 'grounds for suspicion' category which provides a more comprehensive presentation of statistical data in line with international standards of recording data. However, although some SARs may appear similar, an in depth analysis of each SAR will determine the most appropriate grounds for suspicion to be recorded.

As the majority of SARs reported relate to suspected Money Laundering and Fraud related offences as detailed above, further data analysis was undertaken to provide insights into the grounds for suspicion that resulted in SAR disclosures.



MONEY LAUNDERING

SARs raised by principal grounds for suspicion - Money Laundering



Of the Money Laundering SARs reported by MLROs, adverse open source due diligence and inadequate/failure to provide due diligence remains the most common grounds for suspicion, with a very small number of SARs reported with drug trafficking.

**Number of Money Laundering SARs raised by regulated entity**

Regulated entity	2018		2019		2020	
	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported
Insurance Entity 3	20	83.33%	-	-	-	-
Insurance Entity 2	1	4.17%	2	100%	-	-
Insurance Entity 5	2	8.33%	-	-	-	-
Insurance Entity 6	1	4.17%	-	-	-	-
Total	24	100%	2	100%	-	-

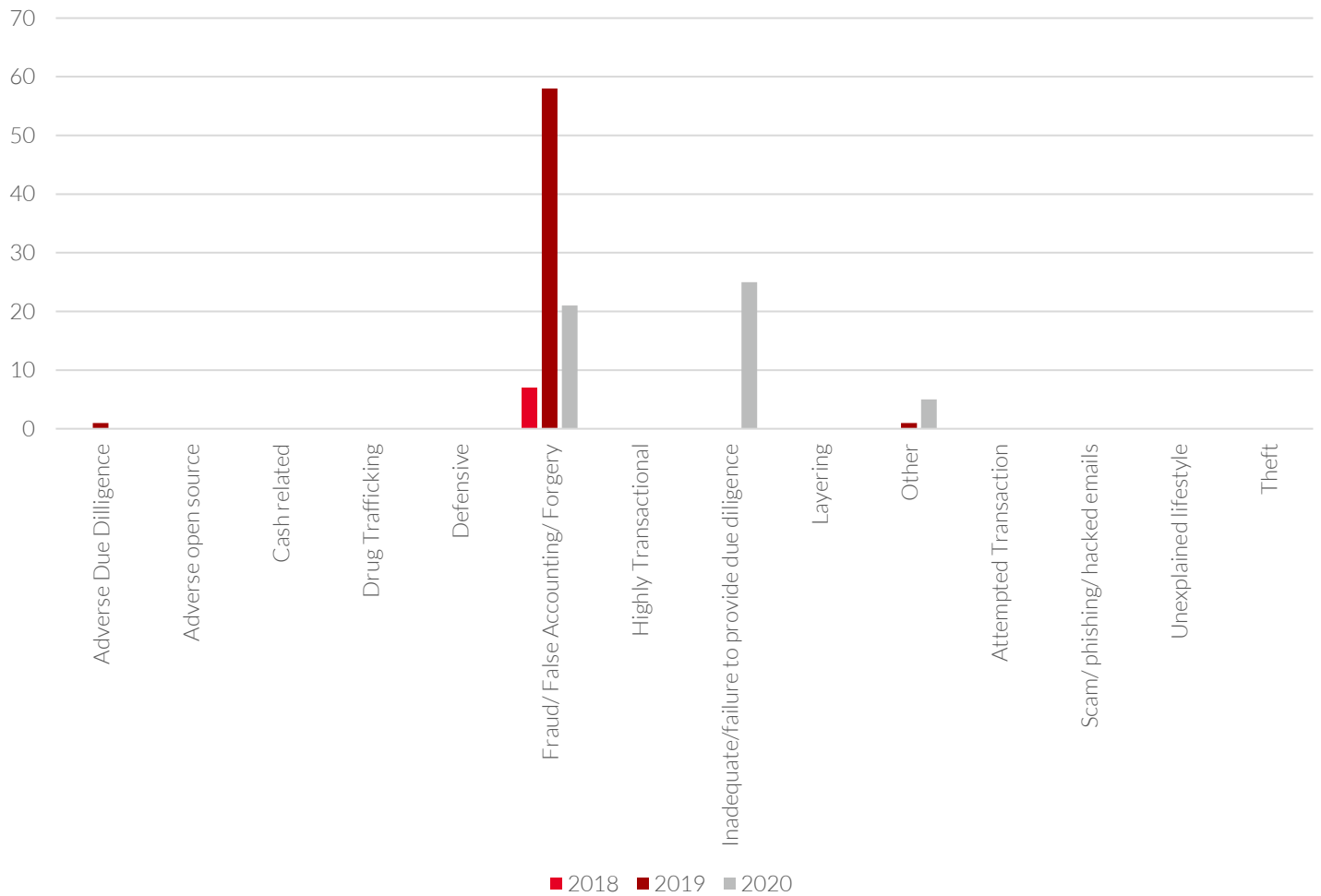
Analysis of the Money Laundering SARs across 2018 and 2019 (with none occurring in 2020), shows that the majority of those reported in 2018 were received from a single company. A number of SARs reported by this company were submitted as a follow-up to a previous SAR, which would suggest that insufficient/inadequate information had been initially reported to the GFIU or the MLRO was unaware of how to update existing SARs.

The significant reduction in Money Laundering SARs reported from 2019 is in contrast to a similar increase by the number of Fraud SARs in the same period. This is attributed to a firm submitting Money Laundering SARs in 2018, which is no longer reporting, and the firm submitting Fraud SARs in 2019 and 2020 not having submitted SARs in 2018. The Fraud SARs are analysed in detail in the next section.



FRAUD

SARs raised by principal grounds for suspicion - Fraud



As detailed earlier in the chapter, there was a significant reduction in the number of SARs reported in relation to Money Laundering in 2019, which has been offset, with a large increase in SARs relating to Fraud. This change in reporting is attributed to different firms reporting in the different years. False accounting/forgery is the most common type of fraud, with firms reporting the use of fraudulent documents in respect of motor vehicle insurance policies as the most common incidence in a Fraud SAR.



Number of SARs raised by regulated entity with grounds of suspicion recorded as Fraud/False Accounting/Forgery

Regulated entity	2018		2019		2020	
	Number of Fraud SARs reported	Percentage of Total Fraud SARs reported	Number of Fraud SARs reported	Percentage of Total Fraud SARs reported	Number of Fraud SARs reported	Percentage of Total Fraud SARs reported
Insurance Entity 1	6	85.71%	-	-	-	-
Insurance Entity 4	1	14.29%	-	-	-	-
Insurance Entity 7	-	-	58	100%	21	100%
Total	7	100%	58	100%	21	100%

Following a similar trend as reported in the Money Laundering analysis above, the distribution of SARs across the industry is unbalanced, with a single firm representing 86% of all Fraud SARs in 2018 and another firm accounting for 100% of all Fraud SARs in 2019 and 2020.

Analysis of the data suggests that insurance intermediaries and insurance managers are most likely to report SARs; this may be attributed to their direct processing of client information in contrast to insurance companies, which often rely on these third parties to perform AML/CFT processes on their behalf. However, given the number of companies in the sector and taking into account the size of the UK car insurance market, only one insurance intermediary is submitting SARs, which raises the possibility that the sector may not be aware of their reporting obligations.

In order to aid MLROs in understanding the typologies that may present in the Insurance sector relating to the following examples are of importance to note:

- Potential new clients are reluctant to provide identity details, disclose source of funds or cooperate in any way;
- Inconsistencies in the information provided by clients pertaining to their business or personal activities and source of wealth;
- Policyholder appears to have no legitimate interest in the insured risk, and policies are entered into without an economic rationale for doing so;
- Individuals seeking to pay large “top-ups” into an existing life insurance policy;
- Purchasing a general insurance policy, then making a claim soon after;
- Where the client appears more interested in learning about cancellation terms rather than about the benefits of the policy;
- Policies cancelled shortly after initiation, especially during the cooling-off period; and
- Individual attempts to seek out insurance for a property or vehicle which does not fit their economic profile.

These examples are not exhaustive but should provide the reader with an understanding of the types of suspicious behaviour that could indicate a need for a SAR to be reported to the GFU.

**Defensive SARs**

	2018		2019		2020	
	Yes	No	Yes	No	Yes	No
GFIU conclusion						
Defensive SAR	1	35	16	53	10	40

As described earlier in the chapter, the data analysis undertaken aimed to assess whether there was a culture of defensive SARs submitted to the GFIU by the Gibraltar Insurance sector. A defensive SAR arises where an activity or a transaction is deemed not suspicious upon further analysis by the GFIU. SARs are required to be filed when a transaction or an attempted transaction involve funds derived from any illegal activity, or when the transaction has no apparent lawful purpose. As the number of SARs received within the Insurance sector have increased significantly over the periods analysed, the analysis above attempts to assess whether the number of defensive SARs raised has also increased. Many entities are wary to be seen by both the GFIU and by their regulator as being complacent or soft on potential instances of Money Laundering. As regulatory and legal scrutiny has increased in this area, so has the risk of regulatory and reputational risk to these entities and so the number of SARs deemed to have been filed in a defensive manner are likely to be explained by this. However, it is important to note that the volume of additional workload created by these defensive SARs where no suspicious activity is contained within have a negative impact on the GFIU, and may even lead to a dilution on the value of SAR reporting as a whole.

Links to Politically Exposed Persons (“PEPs”)

	2018		2019		2020	
	Yes	No	Yes	No	Yes	No
GFIU conclusion						
Link to PEP	-	36	-	69	-	50

The above analysis suggests that there is very little evidence of SARs raised by Insurance entities containing a link to a PEP. This is reported by the MLROs when raising an SAR and both regulations and legal frameworks within Gibraltar require that EDD be applied to all PEPs, including immediate family and known close associates. For any client deemed to be a PEP, specific approval must be obtained for the account opening to continue, the source of funds/wealth must be established and enhanced ongoing monitoring must be applied to the account.



Investment/ Fund Managers/ Securities Sector





BACKGROUND TO THE SECTOR

Gibraltar has a varied Investment/Fund Managers/Securities sector, which cater primarily to non-resident clients. The sector is heavily regulated which is thought to mitigate some of the known risks within the sector. Excluded from regulation are private funds, which are restricted to identifiable categories and carry specific legal requirements.

Investment/Fund Managers are well known for their speed in executing transactions, global reach and adaptability, making the sector attractive to those who may wish to abuse it for illicit purposes. The funds sector mainly focuses on experienced investor funds and private funds locally, both of which are regulated either by the GFSC or have specific legal restrictions applied to them, in order to mitigate potential Money Laundering risks.

For the purposes of this report, Investment/Fund management will be used to define the sector, which consists of investment management companies, the funds sector and securities dealing.

The NRA 2020 rated the Money Laundering threat of the securities and funds sectors as follows:

- Medium Low Risk for Securities;
- Medium Low Risk for Experienced Investor Funds; and
- Medium High Risk for Private Funds.

RESULTS OF DATA ANALYSIS

The data analysis exercise was undertaken in order to analyse the SARs submitted by entities within the sector during the years January – December 2018, 2019 and 2020.

The results have been included below.

Number of regulated entities within the sector

	2018	2019	2020
Fund Administrators	8	7	8
Fund Depositaries	4	4	4
Fund including EIFs	48	48	52
Fund Managers	83	89	83
Investment Firms	25	26	29
Stock Exchange	1	1	1
Total	169	175	177

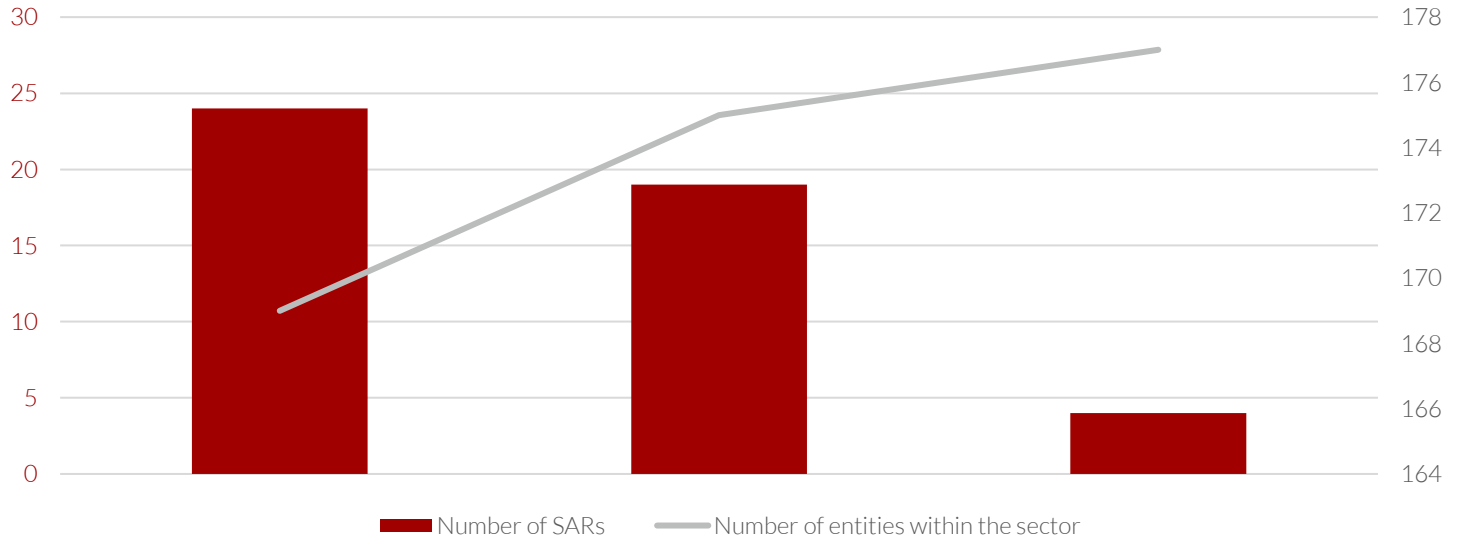


Number of SARs received per Investment/Fund Managers entity

Investment/ Fund Management Entities	2018		2019		2020	
	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported
Investment/Fund Managers entity 1	5	20.83%	-	-	1	25.00%
Investment/Fund Managers entity 2	2	4.17%	-	-	-	-
Investment/Fund Managers entity 3	1	4.17%	-	-	-	-
Investment/Fund Managers entity 4	3	12.50%	-	-	-	-
Investment/Fund Managers entity 5	1	4.17%	-	-	-	-
Investment/Fund Managers entity 6	1	4.17%	-	-	-	-
Investment/Fund Managers entity 7	4	16.67%	-	-	-	-
Investment/Fund Managers entity 8	4	16.67%	-	-	-	-
Investment/Fund Managers entity 9	2	8.33%	-	-	-	-
Investment/Fund Managers entity 10	1	4.17%	-	-	-	-
Investment/Fund Managers entity 11	-	-	11	61.11%	-	-
Investment/Fund Managers entity 12	-	-	4	22.22%	1	25.00%
Investment/Fund Managers entity 13	-	-	2	11.11%	-	-
Investment/Fund Managers entity 14	-	-	1	5.56%	-	-
Investment/Fund Managers entity 15	-	-	-	-	1	25.00%
Investment/Fund Managers entity 16	-	-	-	-	1	25.00%
Total	24	100%	18	100%	4	100%

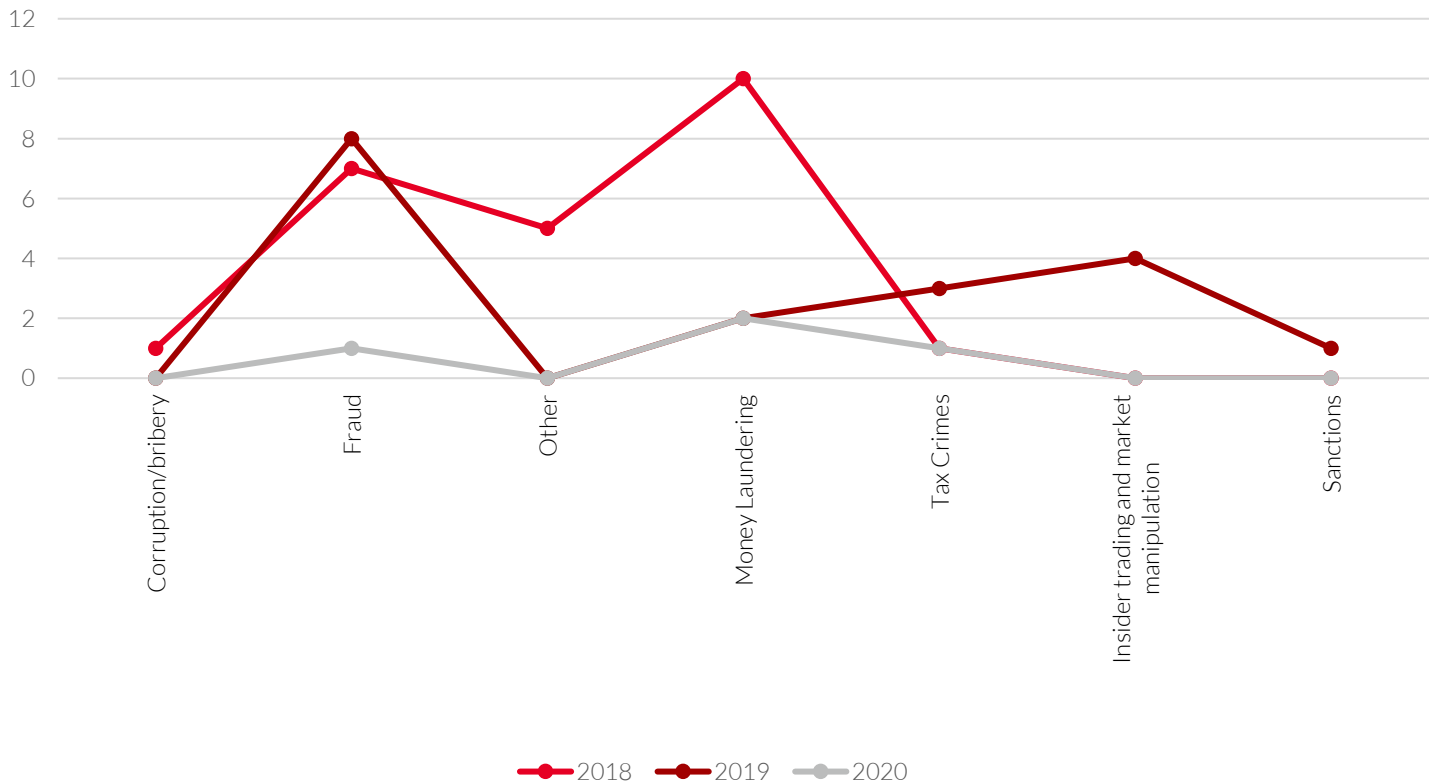


Number of SARs reported vs Number of Entities within the Sector



The number of SARs reported within the sector remained steady across 2018 and 2019, with a significant decrease in 2020 in both the number of SARs reported and the number of firms reporting. As noted, the number of SARs overall reported within the sector is low when considering the number of regulated firms and the level of international work undertaken.

Number of SARs reported by principal suspected criminality





Whilst the number of SARs reported is low, the data above demonstrates that Fraud is the dominant suspected criminality reported by MLROs within Gibraltar's Investment Management sector. There will be SARs where there are multiple suspected criminalities. Themis works on a 'principal crime system', which means that in cases which contain more than one type of offence, it will record the principal suspected criminality. As this is a subjective assessment, there may be inconsistencies between MLROs. There are instances where MLROs have more information than what is included within the SAR, which determines what suspected criminality they record. When there are high risks criminalities like Terrorist Financing, Sexual Exploitation, etc. involved, these should always be recorded as the suspected criminality. There is a spread of suspicious behaviours reported and these have been analysed further below..

GROUNDINGS FOR SUSPICION

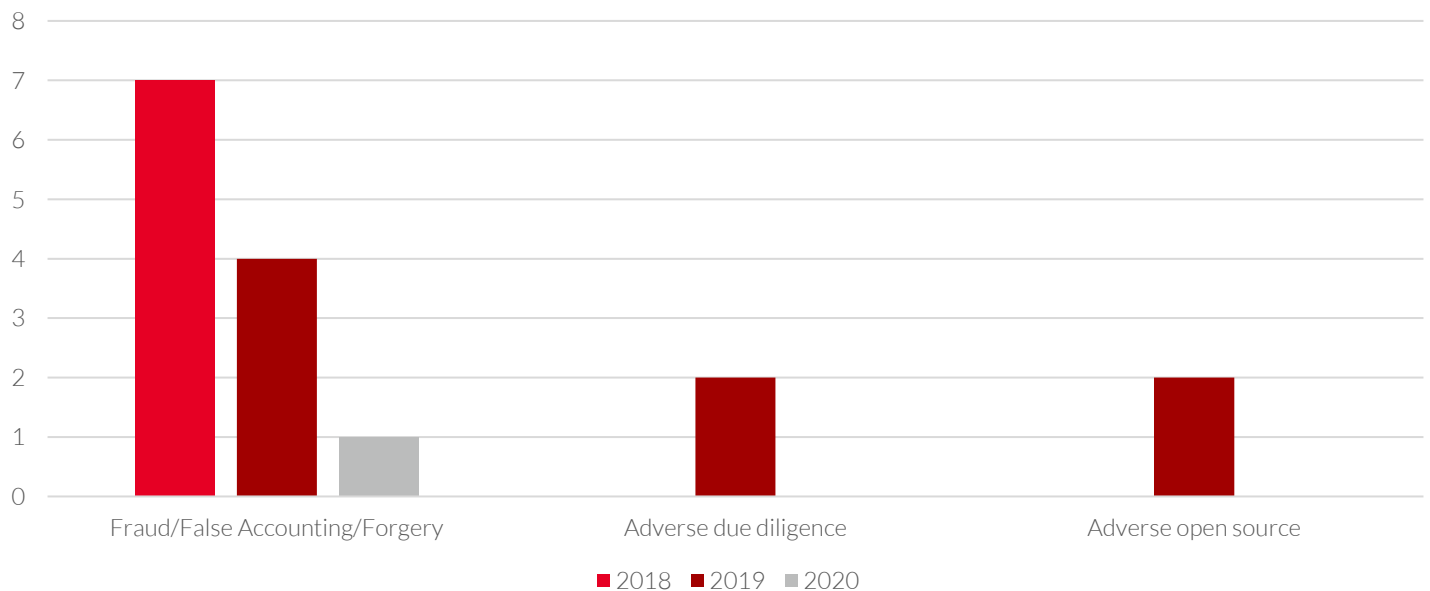
As is the case with suspected criminality, there are SARs which have multiple grounds for suspicion. During the operational analysis of the SAR, the GFIU will record the principal grounds for suspicion. The GFIU's internal Themis system is designed to select one 'grounds for suspicion' category which provides a more comprehensive presentation of statistical data in line with international standards of recording data. However, although some SARs may appear similar, an in depth analysis of each SAR will determine the most appropriate grounds for suspicion to be recorded.

The narrative of the SAR will include all the grounds for suspicion and these are searchable by key words.

As the majority of SARs reported relate to suspected fraud related offences as detailed above, further data analysis was undertaken to provide insights into the grounds for suspicion that resulted in SAR disclosures.

FRAUD

SARs raised by grounds of suspicion - Fraud



During the periods analysed, the highest reported SARs related to the sector reporting fraud, false accounting or the forgery of submitted documents, which resulted in a suspicion.

The below will focus on some of the most frequently evidenced reasons for reporting.



Number of SARs raised by regulated entity with grounds of suspicion recorded fraud, false accounting or forgery.

During the periods analysed, SARs pertaining to fraud, false accounting or forgery were reported most highly. Given the speed with which funds can be transferred within the sector, and its multi-national reach, the sector must be vigilant at all times and report any suspicious activity where necessary. The sector should ensure that at both the onboarding and ongoing monitoring stages of a client relationship, any documentation obtained can be verified independently, and that rationale provided for investment decisions can be supported.

In order to aid MLROs in understanding the typologies that may present in the sector relating to fraud, the following examples are of importance to note:

- Searches on a client or associate show, for example, adverse media attention, disqualification as a director, convictions for dishonesty or association with fraudulent schemes;
- Searches indicate connections to politically exposed persons or their family members which were not disclosed;
- Where the client is, or appears to be, acting on behalf of another person, an unwillingness to give the names of the persons they represent;
- The person acting as a director or representative does not appear to be a suitable representative or does not appear to have the expertise that the role requires;
- Frequent changes in ownership, officers, beneficiaries or trustees in an attempt to evade detection of any potential adverse information available;
- Customer unwilling or refusing to provide information including documentary proof of himself or the beneficial owners;
- Customer carries out transactions for themselves or on behalf of the company that does not correspond with their background;
- The client is secretive about the reasons for and way a company structure is being set up;
- The client's main business rationale is to engage with jurisdictions with, for example, weak anti Money Laundering laws or controls, limited corporate registration requirements, where there is no requirement to update ownership changes, limited beneficial ownership information requirements;
- The client engages in investment decisions with no clear business rationale;
- The client engages in activity considered unusual when compared to their normal activity;
- The client provides inconsistent information such as multiple tax identification numbers, authorisation details or unverified documents;
- The client provides investment documentation which is deemed to be potentially fraudulent; and
- The client attempts to withdraw or release funds with immediacy, or in a timescale considered out of the normal ranges for these types of transactions.

These examples are not exhaustive but should provide the reader with an understanding of the types of suspicious behaviour relating to adverse open source information that could indicate a need for a SAR to be reported to the GFIU.

Generic typologies relevant to the fund and investment sector.

As the volume of SARs reported during the periods analysed was low, this section aims to provide typologies relevant to the investment management sector. These aim to aid MLROs in understanding and assessing potential transactions for red flag indicators, which may require a SAR to be filed.

**Country/geographic risk**

- Clients with relationships identified by credible sources as providing funding or support for terrorist activities or that have terrorist organisations operating within them;
- Clients with relationships identified by credible sources as having significant levels of crime, corruption including illegal drugs, human trafficking, smuggling, illegal gambling etc.;
- Clients with relationships to countries subject to sanctions, embargoes etc.; and
- Clients with relationships identified by credible sources as having weak governance, law enforcement and regulatory regimes.

Client risk

- PEPs and persons closely associated with or related to PEPs who are considered as higher risk clients;
- Clients wanting to conduct or conducting their business in unusual or unconventional circumstances (when compared to known behaviours);
- Clients that are cash intensive businesses;
- Clients with businesses that are not normally cash intensive but appear to have substantial amounts of cash;
- Clients who appear to actively and inexplicably avoid face-to-face meetings or who provide instructions intermittently without legitimate reasons; and
- Clients who request that transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation for accelerating the transaction.

Transaction risk

- Clients who may request that the investment managers represent or assure the client's good standing, reputation and credibility to third parties, without a commensurate knowledge of the client's affairs;
- Clients seeking to acquire investments with no apparent legal, tax, business, economic or other legitimate reason;
- Suspicions held over fraudulent transactions or transactions improperly accounted for etc.

These examples are not exhaustive but should provide the reader with an understanding of the types of suspicious behaviour that could indicate a need for a SAR to be reported to the GFIU within the investment management sector.

**Defensive SARs**

	2018		2019		2020	
GFIU conclusion	Yes	No	Yes	No	Yes	No
Defensive SAR	-	24	4	15	-	4

The data analysis undertaken aimed to assess whether there was a culture of defensive SARs submitted to the GFIU by the sector. A defensive SAR arises where an activity or a transaction is deemed not suspicious upon further analysis by the GFIU. SARs are required to be filed when a transaction or an attempted transaction involve funds derived from any illegal activity, or when the transaction has no apparent lawful purpose. Many entities are wary to be seen by both the GFIU and by their regulator as being complacent or soft on potential instances of Money Laundering. As regulatory and legal scrutiny has increased in this area, so has the risk of regulatory and reputational risk to these entities and so the number of SARs deemed to have been filed in a defensive manner generally can be explained by this. The data analysis above demonstrates that there are low numbers of SARs reported in a defensive manner within the investment management sector.

Links to Politically Exposed Persons (“PEPs”)

	2018		2019		2020	
GFIU conclusion	Yes	No	Yes	No	Yes	No
Link to PEP	2	22	-	19	-	4

The above analysis suggests that there is very little evidence of SARs raised by the sector containing a link to a PEP, which is consistent with the other sectors analysed previously. This is reported by the MLROs when raising a SAR and both regulations and legal frameworks within Gibraltar require that EDD be applied to all PEPs, including immediate family and known close associates. For any client deemed to be a PEP, specific approval must be obtained for the account opening to continue, the source of funds/wealth must be established and enhanced ongoing monitoring must be applied to the account.



Accountants, Auditors and Insolvency Practitioners Sector





BACKGROUND TO THE SECTOR

Auditors certify information by giving an independent expert opinion to improve an organisation's information or its context. In the case of a statutory audit, they provide a legally mandated check of the financial and form an opinion on them. In some instance, they can provide additional services. The Gibraltar Financial Services Commission ("GFSC") licences and regulates both audit firms and individual auditors, however most licenced individuals work at a licenced audit firm.

Insolvency practitioners are charged with the orderly winding down of a firm's activities through a variety of services, which include liquidations, administrations, receiverships, arrangements and bankruptcy proceedings. The practitioner's work involves dealing with many competing interests, but usually their main duty is to look after the interests of creditors. Although creditors can give details of their claims, practitioners will not agree the claims until they are sure that funds will be available. Similar to auditors, insolvency practitioners are regulated by the GFSC and most practitioners are accountants or insolvency specialists working in firms of accountants.

As for all other legal activities, risk of infiltration or ownership by organised crime groups is a Money Laundering threat for accountants, auditors and insolvency practitioners. These professionals may be unwittingly involved in the Money Laundering but may also be complicit or wilfully negligent in conducting their client due diligence obligations.

The sector is well established in Gibraltar and firms provide services to small businesses and local clients, and to large multinational businesses with local operations. As such the actual services delivered by accountants and auditors may vary however, the risks they face remain largely consistent.

As noted above, a large number of licenced auditors and insolvency practitioners' work within licenced audit firms, the majority of which are large global audit firms with robust AML/CFT reporting procedures, as such reporting of SARs by these individuals is performed by the licenced firm's MLRO.

The NRA 2020 rated the Money Laundering and terrorist financing threats arising from the sector as low risk. The risks of these activities occurring in Gibraltar are mitigated primarily through the legislative requirements and ethical standards imposed by professional accounting bodies such as the Association of Chartered Certified Accountants and the Institute of Chartered Accountants in England and Wales of which they are required to be members. All auditors based in Gibraltar follow IESBA standards and insolvency practitioners are required to comply with UK ethical standards. Their professional body - The Gibraltar Society of Accountants ("GSA"), represents the Accountants, Auditors and Insolvency Practitioners in Gibraltar.



RESULTS OF DATA ANALYSIS

The data analysis exercise was undertaken in order to analyse the SARs submitted by entities within the sectors during the years January – December 2018, 2019 and 2020.

The results have been included below.

Notes to our analysis:

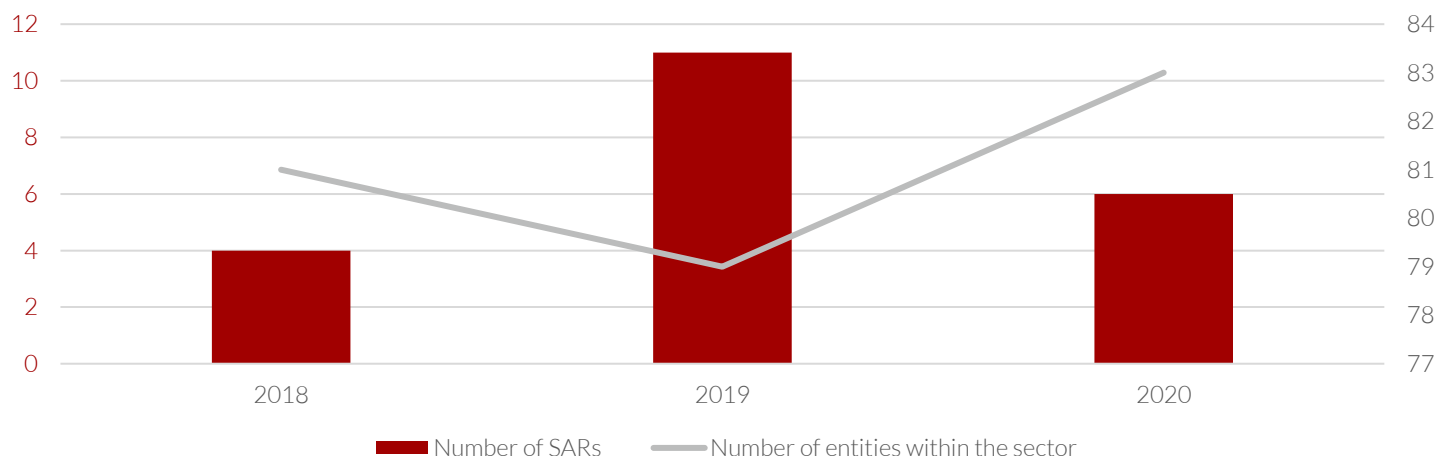
1. Individuals may be licenced as both auditors and insolvency practitioners. The below totals are reflective of the number of active licences in each as they are licenced separately by the GFSC;
2. The number of auditors included below reflects the number of licenced individuals rather than the number of licenced audit firms; and
3. A number of auditors and insolvency practitioners also hold licences within other regulated sectors, such as TCSPs, legal firms, investments and funds firms. There are individuals or firms who have an associated regulated business that will have submitted single SARs in respect of multiple sectors. These SARs are recorded according to the principal reporting entity selected by the MLRO.

Number of licenced auditors and insolvency practitioners within the sector

	2018	2019	2020
Auditors	59	57	59
Insolvency practitioners	22	22	24
Total licenced auditors and insolvency practitioners	81	79	83

Number of SARs received per licenced individual/firm

Licenced individual/firm	2018		2019		2020	
	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported
Auditor/IP Entity 1	2	50.00%	-	-	-	-
Auditor/IP Entity 2	1	25.00%	1	9.09%	-	-
Auditor/IP Entity 3	1	25.00%	-	-	-	-
Auditor/IP Entity 4	-	-	8	72.73%	3	50.00%
Auditor/IP Entity 5	-	-	1	9.09%	1	16.67%
Auditor/IP Entity 6	-	-	1	9.09%	-	-
Auditor/IP Entity 7	-	-	-	-	2	33.33%
Total	4	100%	11	100%	6	100%

**Number of SARs reported vs Number of Entities within the Sector**

The increase in the number of SARs raised 2019, is directly attributable to the number of SARs raised by a single firm, as the number of SARs across the rest of the sector has been consistent year on year. Since 2019, a single firm represented over 50% of SARs.

The number of SARs received from the remaining entities are minimal by comparison and with the sector remaining stable throughout the period under review, the trend raises various questions as to the identification and reporting of potentially suspicious behaviour within the industry.

- Are there common grounds for suspicion driving the reporting of SARs across the sector?
- Are SARs reported predominantly 'defensive' or related to PEPs?

In order to present findings to the above questions, further data analysis was undertaken.

Number of SARs reported by principal suspected criminality

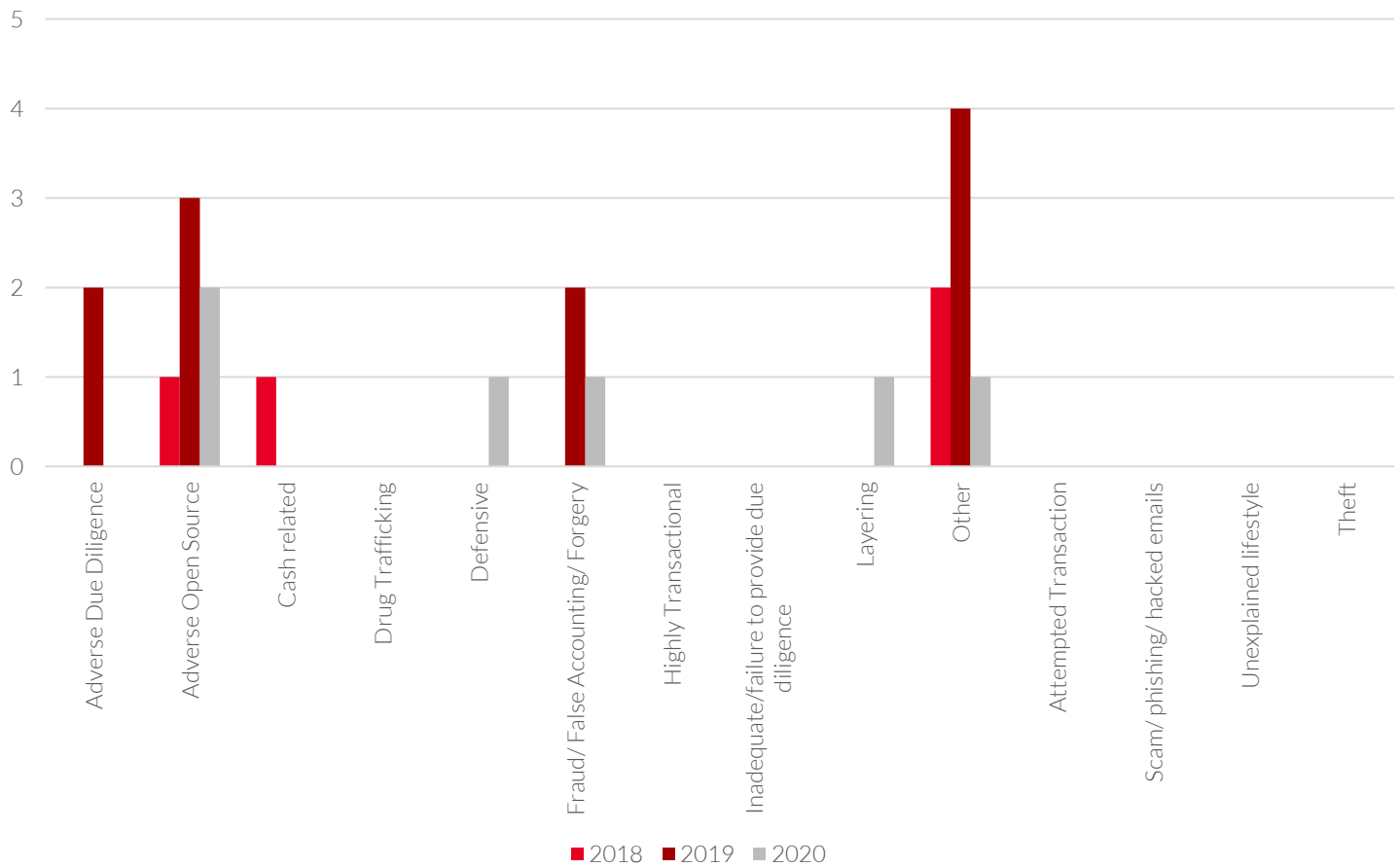
Suspected Criminality	2018		2019		2020	
	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported
Money Laundering	1	25.00%	2	18.18%	5	83.33%
Fraud	-	-	3	27.27%	-	-
Tax Crimes	2	50.00%	4	36.36%	-	-
False Accounting	-	-	-	-	1	16.67%
Terrorism	1	25.00%	-	-	1	16.67%
Corruption	-	-	2	18.18%	-	-
Total SARs	4	100%	11	100%	6	100%

The data above demonstrates that there are no predominant types of suspected criminality in SARs reported to the GFIU by the sector. We have further analysed these below based on the grounds for suspicion detailed in the SARs.



GROUNDS FOR SUSPICION

SARs raised by grounds for suspicion



Of the SARs reported by MLROs, adverse due diligence and adverse open source due diligence remain the most common grounds for suspicion, with a very small number of SARs reported as defensive or relating to Money Laundering or Fraud/ False Accounting/ Forgery.



In order to aid MLROs in understanding the typologies that may present in the Auditors and Insolvency Practitioner sectors relating to due diligence failures, the following examples are of importance to note:

- Potential new clients are reluctant to provide identity details, disclose source of funds or cooperate in any way;
- Inconsistencies in the information provided by clients pertaining to their business or personal activities and source of wealth;
- Clients trying to rush through transactions without providing the requested additional documentation which may be required;
- Clients are unable to explain their source of funds satisfactorily or provide contradictory statements;
- Clients who offer false or fraudulent identification, whether evident from the documents alone, from its lack of connection to the client or from its context in relation to other documents (e.g. use of ID or documents issued in other names without reasonable explanation);
- Clients attempt to obscure the beneficial ownership of assets. Due diligence could be provided for a front company with the aim for this to be used as a legitimate business to hide criminal activity and create legitimate funds;
- Clients who wish to maintain a number of trustees or clients' accounts that do not appear consistent with their type of business;
- Clients provide false/misleading explanations for due diligence purposes;
- Clients become uncontactable when requests for due diligence are made or questions are posed to them;
- Due diligence provided indicates a potential PEP which had not previously been identified;
- Unrealistic turnover or balances detected upon review of company financial statements, that is not in line with the information held by the TCSP on the activity of the client; and
- Frequent changes to the account address or authorised signatories.

**Defensive SARs**

	2018		2019		2020	
	Yes	No	Yes	No	Yes	No
GFIU conclusion						
Defensive SAR	-	4	2	9	-	6

As described earlier in the chapter, the data analysis undertaken aimed to assess whether there was a culture of defensive SARs submitted to the GFIU by the sector. A defensive SAR arises where an activity or a transaction is deemed not suspicious upon further analysis by the GFIU. SARs are required to be filed when a transaction or an attempted transaction involve funds derived from any illegal activity, or when the transaction has no apparent lawful purpose. As the number of SARs received within the sector have increased significantly over the periods analysed, the analysis above attempts to assess whether the number of defensive SARs raised has also increased. Many entities are wary to be seen by both the GFIU and by their regulator as being complacent or soft on potential instances of Money Laundering. As regulatory and legal scrutiny has increased in this area, so has the risk of regulatory and reputational risk to these entities and so the number of SARs deemed to have been filed in a defensive manner are likely to be explained by this. However, it is important to note that the volume of additional workload created by these defensive SARs where no suspicious activity is contained within have a negative impact on the GFIU, and may even lead to a dilution on the value of SAR reporting as a whole.

Links to Politically Exposed Persons (“PEPs”)

	2018		2019		2020	
	Yes	No	Yes	No	Yes	No
GFIU conclusion						
Link to PEP	-	4	-	11	-	6

The above analysis suggests that there is very little evidence of SARs raised by entities containing a link to a PEP. This is reported by the MLROs when raising an SAR and both regulations and legal frameworks within Gibraltar require that EDD be applied to all PEPs, including immediate family and known close associates. For any client deemed to be a PEP, specific approval must be obtained for the account opening to continue, the source of funds/wealth must be established and enhanced ongoing monitoring must be applied to the account.



Money Service Businesses and Money Value Transfer Services Sector





BACKGROUND TO THE SECTOR

Money Service Businesses (“MSBs”) and Money Value Transfer Services (“MVTs”) firms includes those that operate as currency exchanges and provide services to transfer funds or provide payment services.

Currency exchanges allow for the conversion of funds from one currency to another at a rate determined by the provider. Such services are predominantly provided in Gibraltar through the exchange of physical money at various Bureaus de Change. The land border with Spain and large number of workers in Gibraltar who reside in Spain (“cross-border workers”) contributes to the popularity of this service in Gibraltar, as there is significant demand for the exchange of currency on a regular basis. The provision of currency exchange services is a regulated activity, overseen by the Gibraltar Financial Services Commission (“GFSC”). Either the majority of transactions processed in Gibraltar are of small value by tourists or regular amounts exchanged by cross-border workers (e.g. weekly wages) and established businesses. The ML/FT risks posed by this service is further reduced by threshold imposed by the GFSC on licensees to perform due diligence on all transactions in excess of €5,000, a threshold which is lower than required by EU directives.

MVTs refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTs provider belongs. The provision of MVTs is also a regulated activity, overseen by the Gibraltar Financial Services Commission (“GFSC”).

Several features of the sector make these services an attractive vehicle through which criminal and terrorist funds can enter the financial system. These include: the simplicity and certainty of such transactions, worldwide reach (in case of money remitters), the cash character of transactions, the less stringent client identification rules that apply to such transactions compared with opening bank account and reduced possibilities for verification of the client’s identification in comparison to those by credit or other financial institutions. The nature of the client’s relationship with the service provider and the brevity of contacts is also a significant vulnerability.

MSBs and MVTs businesses may be used at all stages of the Money Laundering process. Currency exchanges specifically are an important link in the Money Laundering chain, particularly during the placement stage. Once the money has been exchanged, it could be challenging to trace its origin. Also, it has been noted that considering that they are small businesses, currency exchanges can be easily prone to takeover by criminals and used to launder money.

The nature of MSBs and MVTs businesses are that service providers often carry out one-off transactions with occasional clients, and many of the client relationships that do exist are not of a durable nature. In the case of one-off transactions, some MSBs and MVTs service providers are not able to monitor the financial behaviour of their clients in the same way as a traditional bank is able to do with its clients.

The NRA 2020 rated the Money Laundering and terrorist financing threats arising from the sector as Medium Low Risk. The risks of these activities occurring in Gibraltar are mitigated primarily through the legislative requirements and supervisory measures imposed by the regulator.



RESULTS OF DATA ANALYSIS

The data analysis exercise was undertaken in order to analyse the SARs submitted by entities within the MSBs and MVTs sectors during the years January – December 2018, 2019 and 2020.

The results have been included below.

A number of MSBs are agents of non-Gibraltar based MVTs.

Number of licenced firms within the sector

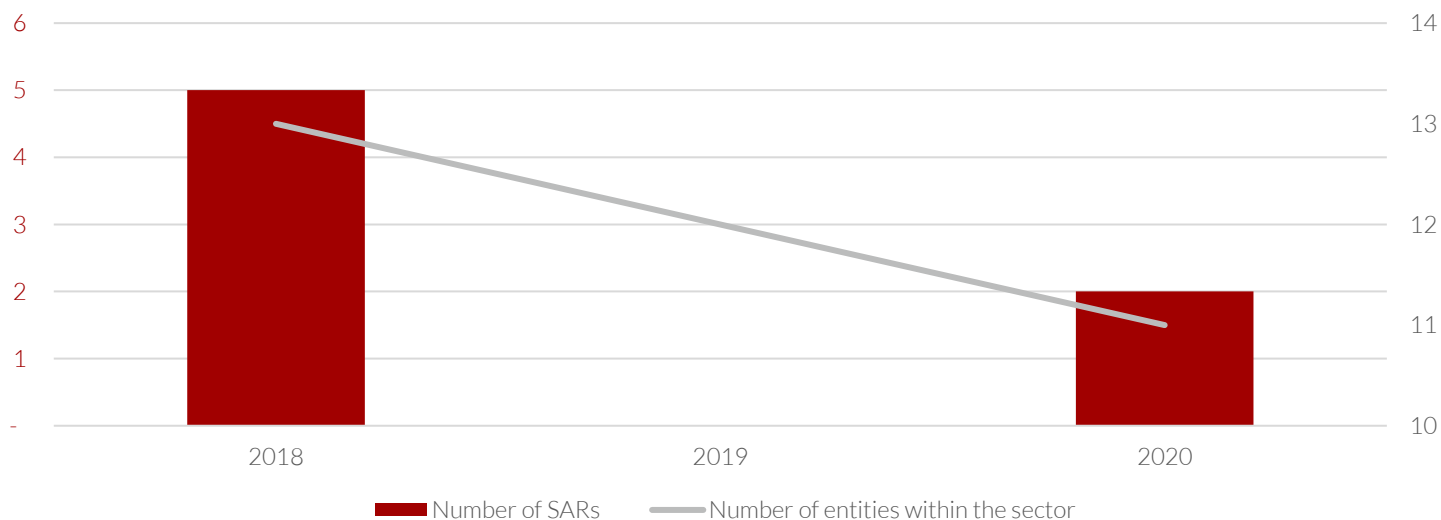
2018	2019	2020
13	12	11

Number of SARs received per licenced firm

Licenced firm	2018		2019		2020	
	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported
MSB/MVT Entity 1	1	20.00%	-	-	1	50.00%
MSB/MVT Entity 2	3	60.00%	-	-	-	-
MSB/MVT Entity 3	1	20.00%	-	-	1	50.00%
Total	5	100%	-	-	2	100%



Number of SARs reported vs Number of Entities within the Sector



The low level of SARs relating to this sector can be attributed to MSBs and MVTs businesses being unable to report any transactions without having oversight of any documentation to prove the clients identity and therefore are unable to report a transaction if it was not completed.

We have further analysed the suspected criminality and grounds for suspicion of SARs reported to the GFIU below to identify whether a commonality in transactions reported exists in the sector.

Number of SARs reported by principal suspected criminality

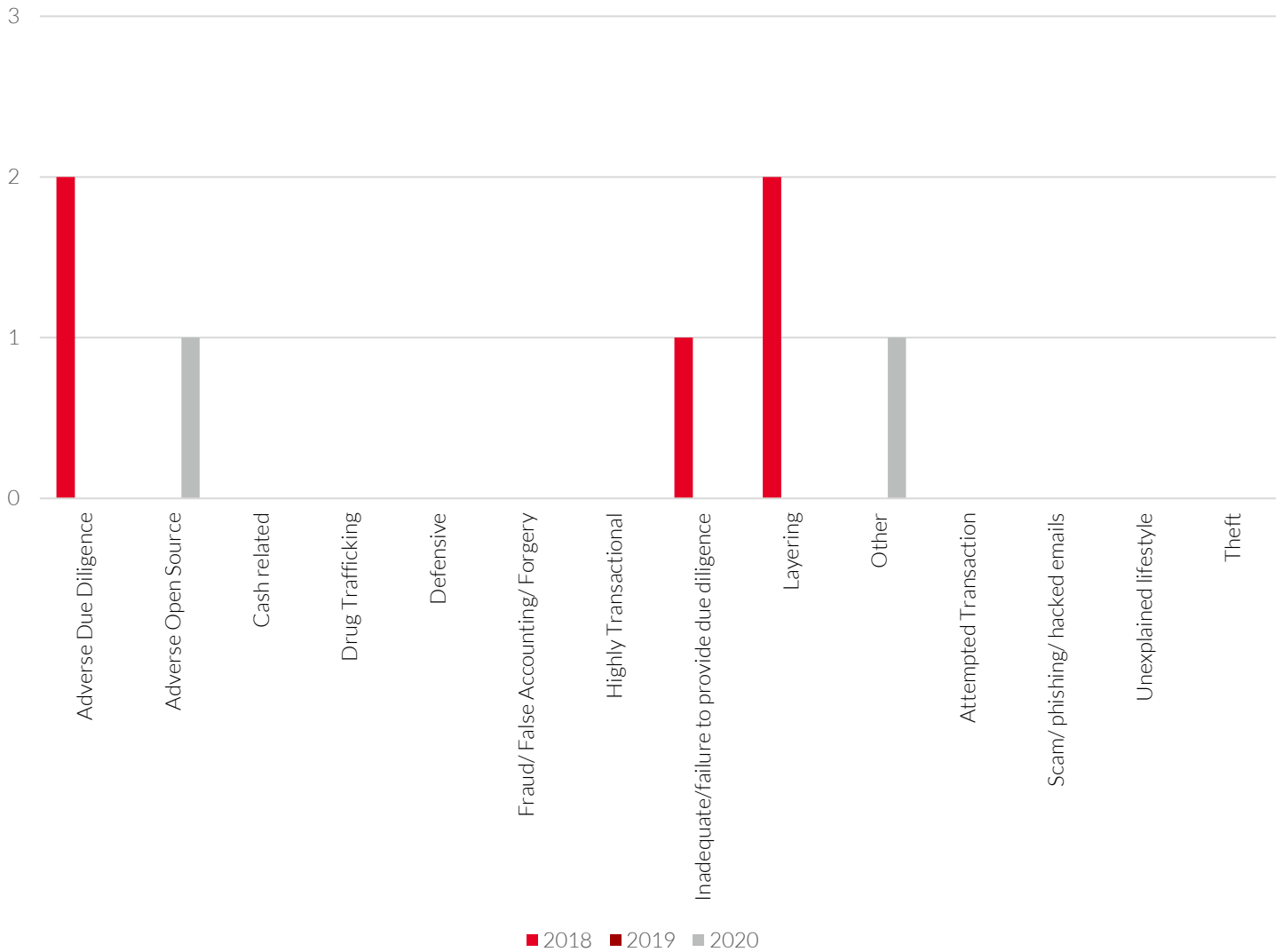
Suspected Criminality	2018		2019		2020	
	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported
Money Laundering	4	80.00%	-	N/A	1	50.00%
Fraud	-	-	-	N/A	1	50.00%
Terrorism	1	20.00%	-	N/A	-	0%
Total SARs	5	100%	-	N/A	2	100%

The data above demonstrates that there are no predominant types of suspected criminality in SARs reported to the GFIU by the sector, this is partly due to the low number of SARs reported. We have further analysed these below based on the grounds for suspicion detailed in the SARs.



GROUNDS FOR SUSPICION

SARs raised by grounds for suspicion



The data above notes that whilst there is not a single predominant ground for suspicion in reporting SARs, due diligence related suspicion is the most common.

We have further analysed the SARs reported below, assessing whether these are ‘defensive’ or related to PEPs.



Defensive SARs

	2018		2019		2020	
	Yes	No	Yes	No	Yes	No
GFIU conclusion						
Defensive SAR	-	5	-	-	-	2

As described earlier in the chapter, the data analysis undertaken aimed to assess whether there was a culture of defensive SARs submitted to the GFIU by the sector. A defensive SAR arises where an activity or a transaction is deemed not suspicious upon further analysis by the GFIU. SARs are required to be filed when a transaction or an attempted transaction involve funds derived from any illegal activity, or when the transaction has no apparent lawful purpose. Our analysis concluded that there were no defensive SARs from this sector.

Links to Politically Exposed Persons (“PEPs”)

	2018		2019		2020	
	Yes	No	Yes	No	Yes	No
GFIU conclusion						
Link to PEP	-	5	-	-	-	2

The above analysis suggests that there is very little evidence of SARs raised by entities containing a link to a PEP. This is reported by the MLROs when raising an SAR and both regulations and legal frameworks within Gibraltar require that EDD be applied to all PEPs, including immediate family and known close associates. For any client deemed to be a PEP, specific approval must be obtained for the account opening to continue, the source of funds/wealth must be established and enhanced ongoing monitoring must be applied to the account.



GENERIC TYPOLOGIES RELEVANT TO THE MSB AND MVTS SECTOR

These aim to aid MLROs in understanding and assessing potential transactions for red flag indicators, which may require a SAR to be filed.

- Client who provides insufficient or suspicious information;
- Client who offers false identification, whether evident from the document alone, from the document's lack of connection to the client, or from the document's context with other documents (e.g., use of identification cards issued by different countries);
- Client who has been the subject of sanctions, known to the MVTS provider;
- Client whose transactions and activities indicate connection with potential criminal involvement or typologies or red flags provided in reports produced by FATF or competent authorities (e.g., the GFIU, the GFSC or the Royal Gibraltar Police) and client whose transaction patterns appear consistent with generation of criminal proceeds;
- Client who transfers funds to or from high risk jurisdictions;
- Activity inconsistent with client's business; and
- Unusual patterns of transactions.

These examples are not exhaustive but should provide the reader with an understanding of the types of suspicious behaviour that could indicate a need for a SAR to be reported to the GFIU within this sector.



10 Legal Professionals and Notaries Sector





BACKGROUND TO THE SECTOR

Gibraltar has a large and varied legal sector and as noted by Moneyval, caters primarily to non-resident clients, although lists of matters provide for the purpose of inspections tend to show that the majority of Relevant Financial Business (“RFB”) is acting for local clients on local property transactions. Lawyers locally act in various capacities and often provide advisory services for other regulated/licensed companies which wish to/or carry out business from Gibraltar. The Proceeds of Crime Act requirements on AML reporting extend to legal professionals where they prepare for or undertake specified RFB activities and do not apply to all activities carried out by a legal professional. The legal sector comprises a broad spectrum of practitioners and for the purposes of this report, includes legal professionals and Notaries. As the range of services provided and carried out by legal professionals is diverse and varies widely, it is important to understand the AML obligations of the sector, and how these services interact with those of other professionals who may have more onerous AML obligations. For the purposes of this report, legal professionals are expected to file a SAR where suspicions are held over a transaction in any of the below areas:

- Buying and selling of real estate;
- Managing of client money, securities or other assets;
- Management of bank, savings or securities accounts;
- Organisation of contributions for the creation, operation or management of companies; and
- Creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

The Proceeds of Crime Act extends requirements for AML checks to be undertaken by legal professionals including client due diligence on the clients themselves, their beneficial owners, and the identification of PEPs as well as ongoing transaction monitoring requirements. It is important to bear in mind when considering the range of tasks undertaken by legal professionals that only the specified activities above are subject to the AML/CFT regime, including the mitigation and management of any potential AML/CFT risks. In Gibraltar, legal professionals frequently work in collaboration with other professional advisors on transactions, such as accountants, TCSPs, real estate agents etc. and may refer their clients to particular professionals for services. Whilst it is common practice for legal firms to hold client funds and to hold these separately from their own, the funds themselves are held with financial institutions and so the flow of funds are dealt with and facilitated by financial institutions, rather than the legal professionals.

For the purposes of this report, legal professionals conducting TCSP activities are considered within the TCSP chapter given that their services are separately licensed and regulated. It is understood that the majority if not all notaries do not carry out RFB or handle client monies and under Gibraltar law, only act to notarise documents and similar functions and so are not considered a high risk.



The NRA 2020 rated the Money Laundering threat of the Legal sector as Medium High Risk for Legal Professionals.

The NRA highlights that legal professionals may inadvertently be involved in Money Laundering schemes via a variety of means. Legal professionals possess a range of specialised legal skills that may be of interest to criminals, in order to enable them to transfer value obtained from criminal activity between parties and obscure ownership. These specialised skills include the creation of financial instruments and arrangements, advice on and drafting of contractual arrangements, and the creation of powers of attorney, all of which have been known to be abused by criminals seeking to launder funds.

For the purposes of this report, legal professionals will be used to denote both legal firms and sole practitioners. Please also note that for the purposes of reporting SARs, legal firms will have employed the majority of the legal professionals issued with practicing certificates. Therefore, it would be the legal firms' respective MLROs who report SARs and not the individual legal professionals themselves.

There are a number of legal firms who have an associated TCSP and that single SARs in respect of both sectors have been submitted by the MLRO. These SARs are recorded according to the principal reporting entity selected by the MLRO.

RESULTS OF DATA ANALYSIS

The data analysis exercise was undertaken in order to analyse the SARs submitted by entities within the legal sector during the years January – December 2018, 2019 and 2020.

The results have been included below.

Number of regulated legal professionals within the sector

	2018	2019	2020
Legal Professionals	39	39	41
Notaries	12	12	12
Total	51	51	53



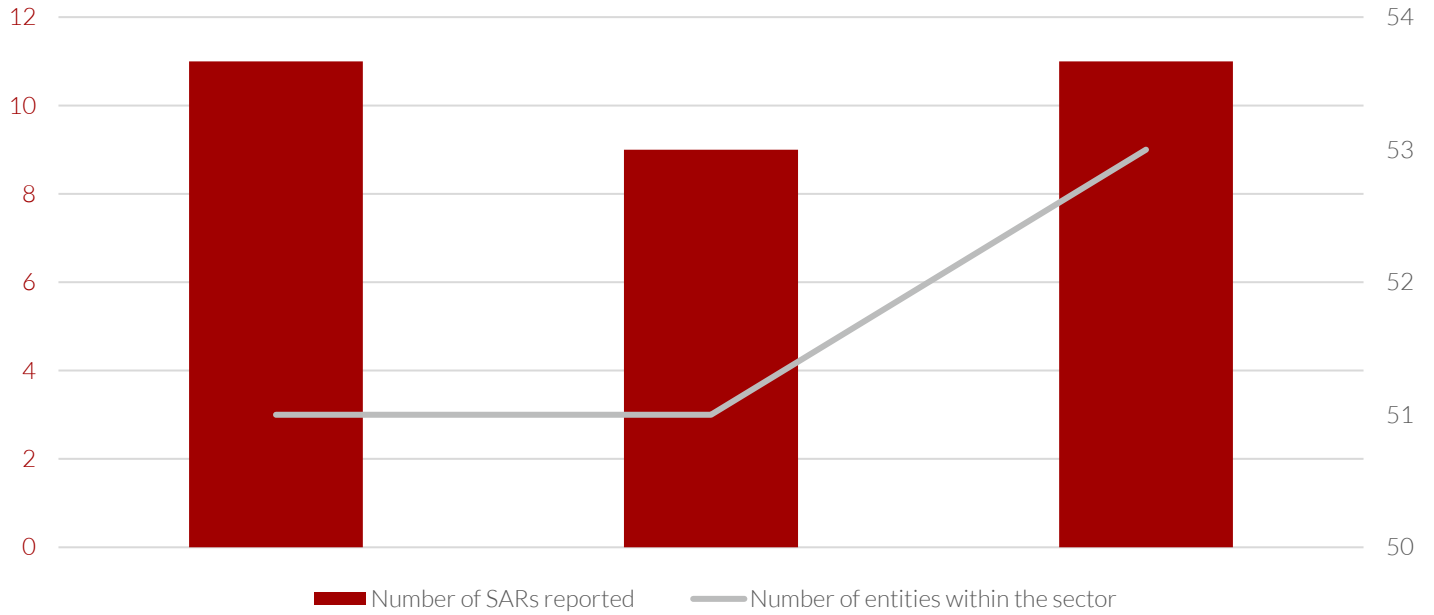
Number of SARs received per legal professionals

Legal professionals	2018		2019		2020	
	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported
Legal Professional/Notary Entity 1	1	9.09%	2	22.22%	1	9.09%
Legal Professional/Notary Entity 2	1	9.09%	-	-	-	-
Legal Professional/Notary Entity 3	1	9.09%	3	33.33%	4	36.36%
Legal Professional/Notary Entity 4	1	9.09%	1	11.11%	-	-
Legal Professional/Notary Entity 5	2	18.18%	-	-	-	-
Legal Professional/Notary Entity 6	1	9.09%	-	-	2	18.18%
Legal Professional/Notary Entity 7	2	18.18%	-	-	-	-
Legal Professional/Notary Entity 8	1	9.09%	-	-	1	9.09%
Legal Professional/Notary Entity 9	-	-	1	11.11%	1	9.09%
Legal Professional/Notary Entity 10	-	-	2	22.22%	1	9.09%
Legal Professional/Notary Entity 11	-	-	-	-	1	9.09%
Legal Professional/Notary Entity 12	1	9.09%	-	-	-	-
Total	11	100%	9	100%	11	100%

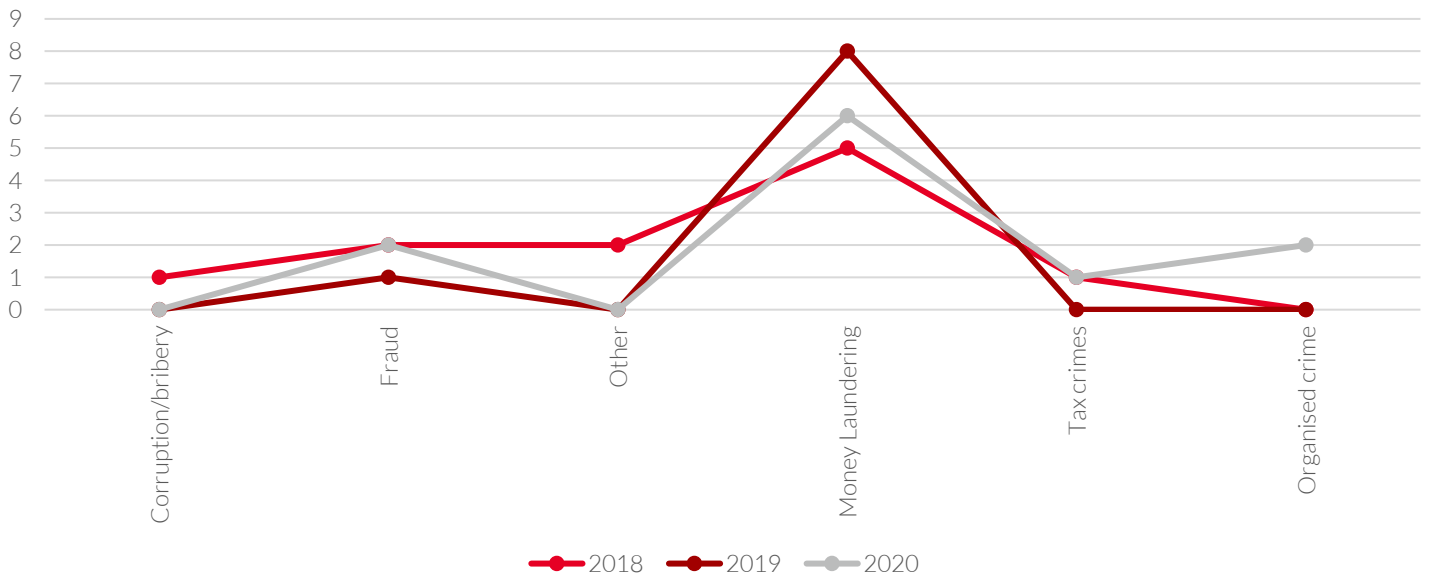
The number of SARs reported remained steady across all periods analysed and was consistent across all professionals. As noted, the number of SARs overall reported within the sector is low when considering the number of legal professionals and the level of international work undertaken.



Number of SARs reported vs Number of Entities within the Sector



Number of SARs reported by principal suspected criminality



Whilst the number of SARs reported is low, the data above demonstrates that Money Laundering is the dominant principal suspected criminality reported by MLROs within the legal sector. There will be SARs where there are multiple suspected criminalities. Themis works on a ‘principal crime system’, which means that in cases which contain more than one type of offence, it will record the principal suspected criminality. There is a spread of suspicious behaviours reported and these have been analysed further below.

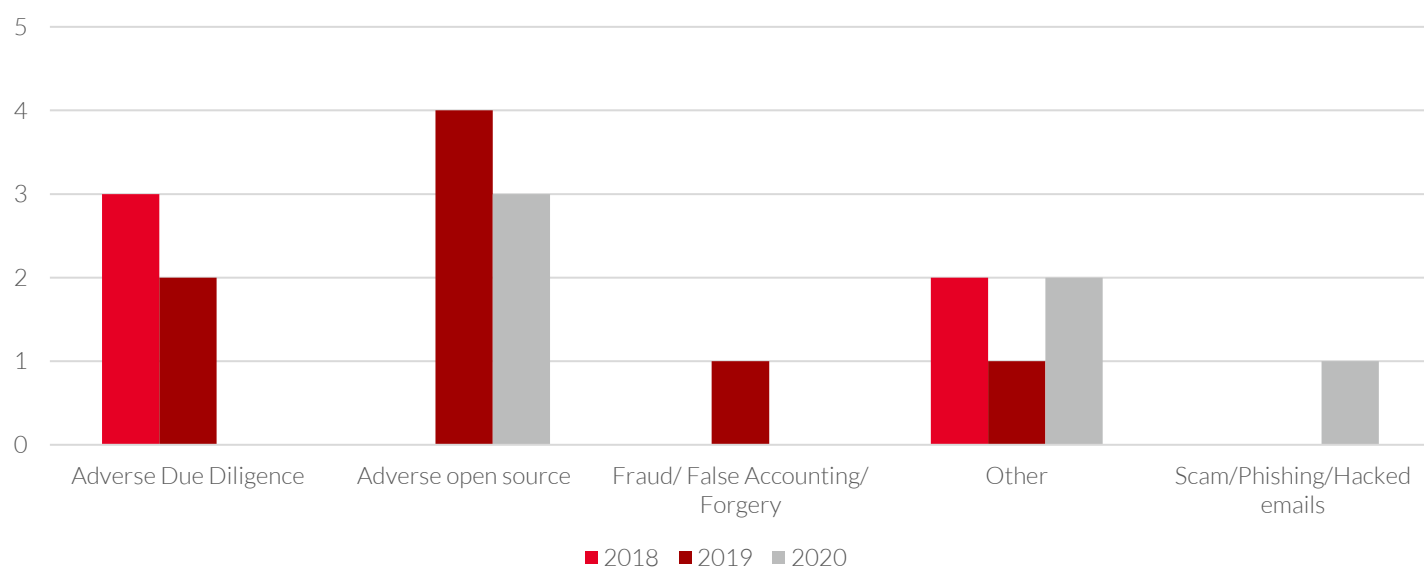


GROUNDS FOR SUSPICION

The majority of SARs reported, relate to suspected Money Laundering related offences as detailed above, further data analysis was undertaken to provide insights into the grounds for suspicion that resulted in SAR disclosures. As is the case with suspected criminality, there are SARs which have multiple grounds for suspicion. During the operational analysis of the SAR, the GFIU will record the principal grounds for suspicion. The GFIU’s internal Themis system is designed to select one ‘grounds for suspicion’ category which provides a more comprehensive presentation of statistical data in line with international standards of recording data.

MONEY LAUNDERING

SARs raised by principal grounds for suspicion - Money Laundering



During the periods analysed, the highest reported SARs related to legal professionals obtaining adverse open source or adverse due diligence information on clients, which resulted in a suspicion.

The below will focus on some of the most frequently evidenced reasons for reporting.

Number of SARs raised by regulated entity with grounds of suspicion recorded as adverse open source or due diligence information.

During the periods analysed, adverse open source or due diligence information was reported highly as the reason legal professionals report a SAR. Legal professionals may not routinely deal directly with a client’s funds, but will be able to focus on the persons they are transacting with and the nature of the services provided. In view of the risks involved, legal professionals must be vigilant at all times and report any suspicious activity where necessary and open source checks provide a useful way of gathering information on clients as part of wider transaction monitoring requirements, and also at the client onboarding stage.



Open source information is information considered widely available, be that via internet searches, social media, the wider online media, the electoral register, sanctions lists, etc. This information is often used to compliment due diligence documentation received and provides the legal professionals with further information into a clients' identity, source of wealth etc. When these reviews are performed, any information which is deemed to be adverse or negative is used to assist the legal professionals in forming a view on the client and whether or not to proceed with the business relationship, or onboard them in the first place.

In order to aid MLROs in understanding the typologies that may present in the legal sector relating to adverse open source information, the following examples are of importance to note:

- Searches on a client or associate show, for example, adverse media attention, disqualification as a director, convictions for dishonesty or association with bribery in relation to contract procurement;
- Searches indicate connections to politically exposed persons or their family members which were not disclosed;
- Where the client is, or appears to be, acting on behalf of another person, an unwillingness to give the names of the persons they represent;
- The person acting as a director or representative does not appear to be a suitable representative or does not appear to have the expertise that the role requires;
- Frequent changes in ownership, officers, beneficiaries or trustees in an attempt to evade detection of any potential adverse information available;
- Customer unwilling or refusing to provide information including documentary proof of himself or the beneficial owners of trusts or companies;
- Customer carries out transactions for themselves or on behalf of the company that does not correspond with their background;
- The beneficial ownership is veiled in complexity making it impossible to determine;
- The client is secretive about the reasons for and way a company structure is being set up;
- The client's main business rationale is to engage with jurisdictions with, for example, weak anti Money Laundering laws or controls, limited corporate registration requirements, where there is no requirement to update ownership changes, limited beneficial ownership information requirements; and
- The client favours legal entities that are not transparent.

These examples are not exhaustive but should provide the reader with an understanding of the types of suspicious behaviour relating to adverse open source information that could indicate a need for a SAR to be reported to the GFIU.



GENERIC TYPOLOGIES RELEVANT TO THE LEGAL PROFESSIONALS SECTOR

As the volume of SARs reported during the periods analysed was low, this section aims to provide typologies relevant to the legal sector. These aim to aid MLROs in understanding and assessing potential transactions for red flag indicators, which may require a SAR to be filed.

Country/geographic risk

- Clients with relationships identified by credible sources as providing funding or support for terrorist activities or that have terrorist organisations operating within them;
- Clients with relationships identified by credible sources as having significant levels of crime, corruption including illegal drugs, human trafficking, smuggling, illegal gambling etc.;
- Clients with relationships to countries subject to sanctions, embargoes etc.; and
- Clients with relationships identified by credible sources as having weak governance, law enforcement and regulatory regimes.

Client risk

- PEPs and persons closely associated with or related to PEPs who are considered as higher risk clients;
- Clients wanting to conduct or conducting their business in unusual or unconventional circumstances (when compared to known behaviours);
- Clients that are cash intensive businesses;
- Clients with businesses that are not normally cash intensive but appear to have substantial amounts of cash;
- Clients who appear to actively and inexplicably avoid face-to-face meetings or who provide instructions intermittently without legitimate reasons; and
- Clients who request that transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation for accelerating the transaction.

Transaction risk

- Clients who may request financial transactions occur outside of client accounts (i.e. the legal professionals own business accounts);
- Clients who may request that legal professionals represent or assure the client's good standing, reputation and credibility to third parties, without a commensurate knowledge of the client's affairs;
- Transfer of real estate or other high value goods between parties in a time period that is unusually short for similar transactions;
- Clients seeking to acquire businesses in liquidation with no apparent legal, tax, business, economic or other legitimate reason;
- Suspicions held over fraudulent transactions or transactions improperly accounted for such as the over or under invoicing of goods/services, falsely described goods/services etc.

These examples are not exhaustive but should provide the reader with an understanding of the types of suspicious behaviour that could indicate a need for a SAR to be reported to the GFIU within the legal sector.

**Defensive SARs**

	2018		2019		2020	
	Yes	No	Yes	No	Yes	No
GFIU conclusion						
Defensive SAR	1	10	2	7	2	10

The data analysis undertaken aimed to assess whether there was a culture of defensive SARs submitted to the GFIU by the legal sector. A defensive SAR arises where an activity or a transaction is deemed not suspicious upon further analysis by the GFIU. SARs are required to be filed when a transaction or an attempted transaction involve funds derived from any illegal activity, or when the transaction has no apparent lawful purpose. As the number of SARs received within the legal sector have remained relatively stable over the periods analysed, the analysis above attempts to assess whether the number of defensive SARs raised has increased over time. Many entities are wary to be seen by both the GFIU and by their regulator as being complacent or soft on potential instances of Money Laundering. As regulatory and legal scrutiny has increased in this area, so has the risk of regulatory and reputational risk to these entities and so the number of SARs deemed to have been filed in a defensive manner generally can be explained by this. The data analysis above demonstrates that there are low numbers of SARs reported in a defensive manner within the legal sector.

Links to Politically Exposed Persons (“PEPs”)

	2018		2019		2020	
	Yes	No	Yes	No	Yes	No
GFIU conclusion						
Link to PEP	1	10	-	9	-	12

The above analysis suggests that there is very little evidence of SARs raised by legal professionals containing a link to a PEP, which is consistent with the other sectors analysed previously. This is reported by the MLROs when raising a SAR and both regulations and legal frameworks within Gibraltar require that EDD be applied to all PEPs, including immediate family and known close associates. For any client deemed to be a PEP, specific approval from senior management must be obtained for the account opening to continue, the source of funds/wealth must be established and enhanced ongoing monitoring must be applied to the account.



11 Real Estate Agents Sector





BACKGROUND TO THE SECTOR

Organised crime groups can use the real estate sector to launder the proceeds of crime and to hide the illegal origin of the funds. Real estate holds its value, can give returns on investment and requires little specific expertise or knowledge which increases its financial attractiveness to criminals.

Gibraltar is a very small country covering an area of approximately 6.8 km. Of this area, approximately 40% consists of the upper rock nature reserve that is a mostly uninhabited protected area. There are approximately 19,200 properties in Gibraltar; of these 3,900 are commercial and of the remaining 15,300 properties, there are four types of residential properties:

1. Government of Gibraltar (“GoG”) rental stock: 100% owned by GoG, let directly by GoG’s Housing Department to Gibraltarians and cannot be sublet (approximately 5,300 properties);
2. Co-ownership properties: Government funded “affordable” properties, subject to a minimum 3 year Gibraltar residency requirement, often co-owned between GoG and the occupier and with rental restrictions (approximately 4,900 properties);
3. Open market properties: not generally subject to restrictions, are available to any owner or occupant and can be rented (approximately 4,800); and
4. Ministry of Defence properties: solely for occupation by the British Forces personal (approximately 300).

The scarcity of land keeps demand and property prices high, which can be attractive to criminals. Only open market and commercial properties however are considered suitable for investment and therefore targets for international criminal groups. This only represents 25% of the residential property market of which the majority are occupied by locals or foreign workers and expats who are not eligible for co-ownership properties. Local criminals eligible for co-ownership properties may however see these attractive although the exchange of funds in such circumstances would be limited and for a single transaction only as eligibility is for one co-ownership property only.

The open market property rental market is attractive for investment due to the big demand for rental accommodation as there is limited rental stock. The opportunities for criminal groups seeking to launder funds on a significant scale however are similarly reduced by lack of availability of properties. The letting of other properties is not deemed attractive for international criminals due to the restrictions on rentals. There may be limited attraction of GoG rental stock and non-declared rental of restricted co-ownership properties to low-level local criminals if they are seeking to rent homes for their own use. However, the exchange of funds in such circumstances would be very small.

Real Estate Agents (“REAs”) include businesses which provide services associated with the buying, selling and leasing of property as defined in the Office of Fair Trading’s (“OFT”) AML/CFT Guidance Notes for REAs. They are subject to anti-Money Laundering requirements and are licensed and regulated by the OFT. REAs are required to carry out CDD on both parties to a real estate transaction before proceeding with the same.



Unlike REAs in other jurisdictions, Gibraltar REAs only receive a commission on the transfer of real estate, which is usually between 1-2% of the purchase price, but do not handle the purchase funds, which are instead handled by lawyers through their client accounts. This substantially decreases the attractiveness to criminals using Gibraltar REAs for laundering and therefore reducing the ML/TF threat as money would not flow through them.

All licensed REAs are required to carry out annual risk assessment of the business, report annually to the OFT and to implement internal systems of control in order to understand and thereafter mitigate their ML/TF risk.

The NRA 2020 rated the Money Laundering threat of the REA sector as follows:

- Medium Low Risk for Real Estate Agents.

RESULTS OF DATA ANALYSIS

The data analysis exercise was undertaken in order to analyse the SARs submitted by entities within the sector during the years January – December 2018, 2019 and 2020.

The results have been included below.

Number of REAs within the sector

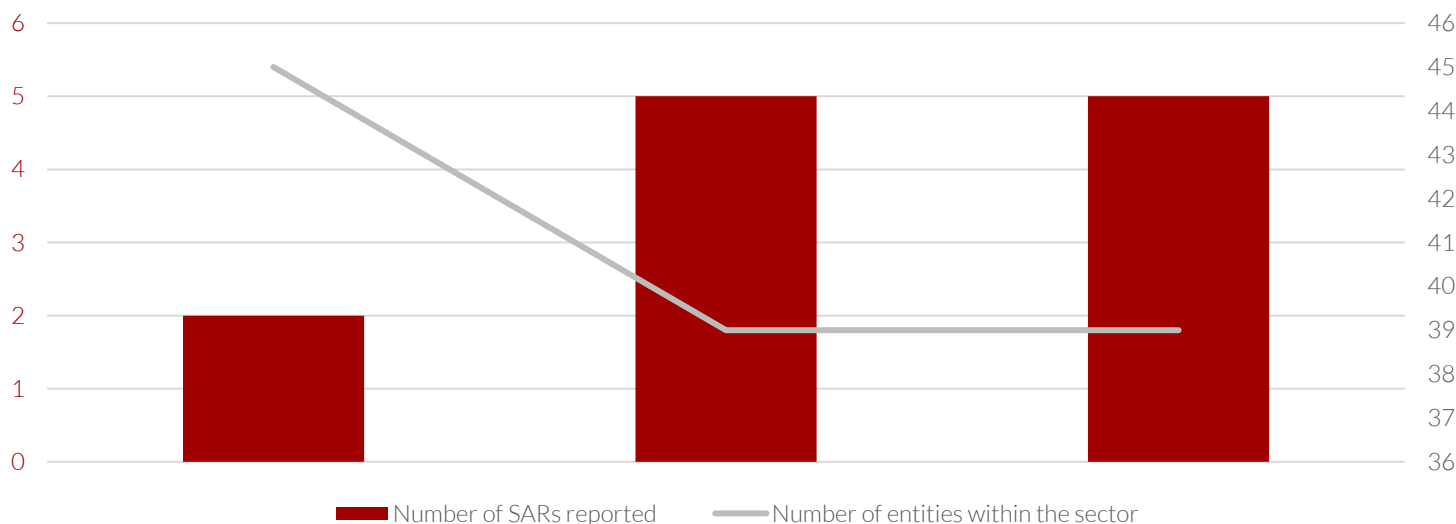
	2018	2019	2020
Real Estate Agents	45	39	39

Number of SARs received per REA

Real estate agency	2018		2019		2020	
	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported
Real Estate Agency 1	1	50.00%	4	80.00%	4	80.00%
Real Estate Agency 2	1	50.00%	-	-	-	-
Real Estate Agency 3	-	-	1	20.00%	1	20.00%
Total	2	100%	5	100%	5	100%



Number of SARs reported vs Number of Entities within the Sector



The number of SARs reported within the sector was extremely low but as identified in the introduction to this chapter, it is thought that many of the AML risks associated with the purchase of real estate are mitigated by other regulated businesses being involved with the transaction and flow of funds. The majority of SARs related to the purchase of properties with a small number reported in respect of rental. The majority of the SARs included consent requests. Although most of the SARs received had other regulated businesses involved in the reported suspicious transaction, the majority of these regulated businesses did not submit a SAR.

Most of the SARs received are from one regulated firm. As noted, the number of SARs overall reported within the sector is low when considering the number of regulated firms and an increase in high net worth individuals purchasing properties in Gibraltar for investment purposes.

Number of SARs reported by principal suspected criminality

Suspected Criminality	2018		2019		2020	
	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported
Money Laundering	2	100%	4	80.00%	5	100%
Fraud	-	-	1	20.00%	-	-
Total SARs	2	100%	5	100%	5	100%

Whilst the number of SARs reported is low, the data above demonstrates that suspected Money Laundering was the dominant suspected criminality reported by MLROs within the sector. The principal ground for suspicion reported was adverse open source on clients, which resulted in a suspicion.

The data provided is limited given the population size and so the typologies identified aim to provide the local REA sector with information on trends and patterns identified within the UK and the EU, which may be relevant to Gibraltar.



GENERIC TYPOLOGIES RELEVANT TO THE REAL ESTATE SECTOR

These aim to aid MLROs in understanding and assessing potential transactions for red flag indicators, which may require a SAR to be filed.

Country/geographic risk

- Clients with relationships identified by credible sources as providing funding or support for terrorist activities or that have terrorist organisations operating within them;
- Clients with relationships identified by credible sources as having significant levels of crime, corruption including illegal drugs, human trafficking, smuggling, illegal gambling etc.;
- Clients with relationships to countries subject to sanctions, embargoes etc.; and
- Clients with relationships identified by credible sources as having weak governance, law enforcement and regulatory regimes.

Client risk

- PEPs and persons closely associated with or related to PEPs who are considered as higher risk clients;
- Clients wanting to conduct or conducting their business in unusual or unconventional circumstances (when compared to known behaviours);
- Clients that are cash intensive businesses or wish to purchase real estate exclusively in cash;
- Clients who rely solely on the use of intermediaries to attempt to hide involvement;
- Clients who appear to actively and inexplicably avoid face-to-face meetings or who provide instructions intermittently without legitimate reasons;
- Searches on a client show, for example, adverse media attention, disqualification as director, convictions of dishonesty etc.; and
- Clients who request that transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation for accelerating the transaction.

Transaction risk

- Clients whose source of funds cannot be verified or is not in keeping with their known client profile;
- Clients are unable or reluctant to provide information about the source of funds or wealth when this is requested;
- Ownership of property is to be through a series of complex legal structures or complex corporate structures for no apparent reason;
- Client requests that the asking price/letting price be unreasonably higher than the valuation suggests;
- Client lets at or sells at a price which is significantly above or below market price, or a transaction which seems uneconomic or inefficient;
- Successive sale transactions, especially of the same property, in a short period of time with unexplained changes in value;
- Clients seeking to acquire property with no apparent legal, tax, business, economic or other legitimate reason;
- Suspicions held over fraudulent transactions or transactions improperly accounted for etc.

These examples are not exhaustive but should provide the reader with an understanding of the types of suspicious behaviour that could indicate a need for a SAR to be reported to the GFIU within the real estate sector.

**Defensive SARs**

	2018		2019		2020	
	Yes	No	Yes	No	Yes	No
GFIU conclusion						
Defensive SAR	-	2	1	4	1	4

The data analysis undertaken aimed to assess whether there was a culture of defensive SARs submitted to the GFIU by the sector. A defensive SAR arises where an activity or a transaction is deemed not suspicious upon further analysis by the GFIU. SARs are required to be filed when a transaction or an attempted transaction involve funds derived from any illegal activity, or when the transaction has no apparent lawful purpose. Many entities are wary to be seen by both the GFIU and by their regulator as being complacent or soft on potential instances of Money Laundering. As regulatory and legal scrutiny has increased in this area, so has the risk of regulatory and reputational risk to these entities and so the number of SARs deemed to have been filed in a defensive manner generally can be explained by this. The data analysis above demonstrates that there are low numbers of SARs reported generally, with low numbers reported in a defensive manner within the real estate sector.

Links to Politically Exposed Persons (“PEPs”)

	2018		2019		2020	
	Yes	No	Yes	No	Yes	No
GFIU conclusion						
Link to PEP	-	2	-	5	-	5

The above analysis suggests that there is no evidence of SARs raised by the sector containing a link to a PEP, which is consistent with the other sectors analysed previously. This is reported by the MLROs when raising a SAR and both regulations and legal frameworks within Gibraltar require that EDD be applied to all PEPs, including immediate family and known close associates. For any client deemed to be a PEP, specific approval must be obtained for the account opening to continue, the source of funds/wealth must be established and enhanced ongoing monitoring must be applied to the account.



High Value Dealers and High Risk Dealers Sector





BACKGROUND TO THE SECTOR

The Proceeds of Crime Act imposes AML/CFT obligations on high value goods dealers where they sell high value goods in cash. Any dealer accepting more than £8,000 in cash for goods (in single or linked transactions) is considered a High Value Dealer (“HVD”). Many businesses in Gibraltar no longer accept cash above £8,000 for goods as a matter of policy reducing the burden on individual businesses. In addition to HVDs, the OFT created a category of High Risk Dealers (“HRDs”) being dealers in goods which the OFT considers to have a higher inherent risk and vulnerability to ML/TF irrespective of whether sales in cash surpass the monetary threshold. These goods are precious stones and metals, car and motorbike dealers, marine craft dealers and antique and art dealers that are traditionally industries attractive to criminals for the purposes of laundering money. These sectors are subject to anti-Money Laundering requirements and are regulated by the OFT.

The NRA concludes that due to the small scale of trading in Gibraltar, the risk of these high value goods being used for ML/TF schemes is mitigated considerably as not many opportunities are presented to ML criminals other than to purchase these items as lifestyle goods for their own use.

The NRA 2020 rated the Money Laundering threat of the HVDs and HRDs sector as follows:

- Low Risk for Artefacts, Art and Antiquities;
- Medium Low Risk for Precious Metals and Stones;
- Medium Low Risk for Car Dealers; and
- Medium Low Risk for Other High Value Goods.



RESULTS OF DATA ANALYSIS

The data analysis exercise was undertaken in order to analyse the SARs submitted by entities within the sector during the years January – December 2018, 2019 and 2020.

The results have been included below.

Number of HVDs and HRDs within the sector

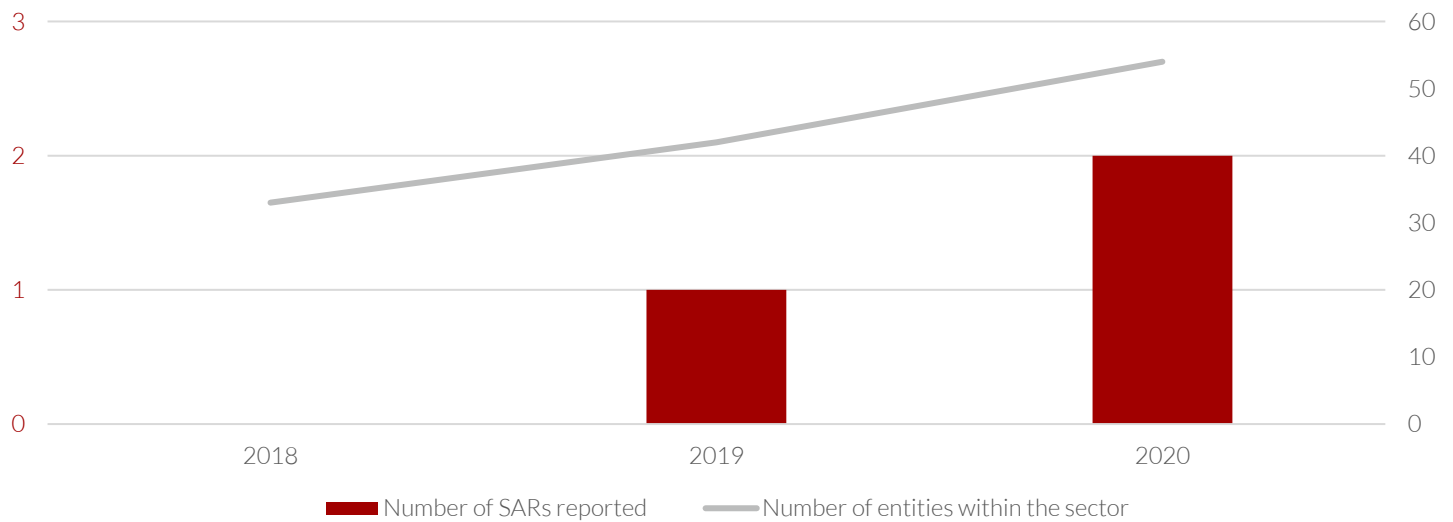
	2018	2019	2020
High Value Dealers	2	4	5
High Risk Dealers	31	38	49
Total	33	42	54

Number of SARs received per HVDs or HRDs

HVD/HRD	2018		2019		2020	
	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported
HVD/HRD Entity 1	-	-	1	100%	-	-
HVD/HRD Entity 2	-	-	-	-	1	50.00%
HVD/HRD Entity 3	-	-	-	-	1	50.00%
Total	-	-	1	100%	2	100%



Number of SARs reported vs Number of Entities within the Sector



The number of SARs reported within the sector was extremely low but as identified in the introduction to this chapter, it is believed that some of the AML risks are mitigated by many businesses in the sector opting to implement cash policies, which do not allow for acceptance of funds over £8,000 in cash as payment. However, the risks to the sector are not limited to cash payments. As noted, the number of SARs overall reported within the sector is low when considering the number of entities within the sector.

Number of SARs reported by principal suspected criminality

Suspected Criminality	2018		2019		2020	
	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported	Number of SARs reported	Percentage of total SARs reported
Money Laundering	-	-	1	100%	2	100%
Total SARs	-	-	1	100%	2	100%

Whilst the number of SARs reported is low, the data above demonstrates that suspected Money Laundering was the sole suspected criminality reported by MLROs within the sector. The data provided is limited given the population size and so the typologies identified aim to provide the local HVD/HRD sector with information on trends and patterns identified within the UK and the EU, which may be relevant to Gibraltar.



GENERIC TYPOLOGIES RELEVANT TO THE HVDS AND HRDS

These aim to aid MLROs in understanding and assessing potential transactions for red flag indicators, which may require a SAR to be filed.

Country/geographic risk

- Cash payments from individuals residing in high-risk jurisdictions which may be more likely to be linked to Money Laundering;
- Cash payments received from clients operating in countries who restrict the use of cash and/or have limits in place for amounts of cash permitted to enter/leave the country;
- Does the transaction make commercial sense? Does the client have a market place for the goods you are selling in their home country?;
- Client risk;
- Clients wanting to conduct or conducting their business in unusual or unconventional circumstances (when compared to known behaviours);
- Clients that are cash intensive businesses or wish to purchase goods exclusively in cash;
- Clients who rely solely on the use of intermediaries to attempt to hide involvement;
- Clients who appear to actively and inexplicably avoid face-to-face meetings or who provide instructions intermittently without legitimate reasons for their purchases;
- Clients seeking to pay for goods exclusively in other currencies such as euros with no area or business links to other jurisdictions; and
- Clients who request that transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation for accelerating the purchase.

Transaction risk

- Client whose source of funds cannot be verified or is not in keeping with their known client profile;
- Uncharacteristic transactions which are not in keeping with the client's financial situation;
- The pattern and or frequency of an existing client has changed since the business relationship was established;
- Clients are unable or reluctant to provide information about the source of funds or wealth when this is requested;
- The person paying the cash is not known to you and does not appear to have a link to the client;
- Client claims not to have a bank account and relies solely on cash to make high value/risk purchases; and
- Unfamiliar or atypical types of client or transaction.

These examples are not exhaustive but should provide the reader with an understanding of the types of suspicious behaviour that could indicate a need for a SAR to be reported to the GFIU within the HRD/HVD sector.

**Defensive SARs**

	2018		2019		2020	
GFIU conclusion	Yes	No	Yes	No	Yes	No
Defensive SAR	-	-	-	1	-	2

The data analysis undertaken aimed to assess whether there was a culture of defensive SARs submitted to the GFIU by the sector. A defensive SAR arises where an activity or a transaction is deemed not suspicious upon further analysis by the GFIU. SARs are required to be filed when a transaction or an attempted transaction involve funds derived from any illegal activity, or when the transaction has no apparent lawful purpose. Many entities are wary to be seen by both the GFIU and by their regulator as being complacent or soft on potential instances of Money Laundering. As regulatory and legal scrutiny has increased in this area, so has the risk of regulatory and reputational risk to these entities and so the number of SARs deemed to have been filed in a defensive manner generally can be explained by this. The data analysis above demonstrates that there are low numbers of SARs reported generally, and none reported in a defensive manner within the HVD/HRD sector.

Links to Politically Exposed Persons (“PEPs”)

	2018		2019		2020	
GFIU conclusion	Yes	No	Yes	No	Yes	No
Link to PEP	-	-	-	1	-	2

The above analysis suggests that there is no evidence of SARs raised by the sector containing a link to a PEP, which is consistent with the other sectors analysed previously. This is reported by the MLROs when raising a SAR and both regulations and legal frameworks within Gibraltar require that EDD be applied to all PEPs, including immediate family and known close associates. For any client deemed to be a PEP, specific approval must be obtained for the account opening to continue, the source of funds/wealth must be established and enhanced ongoing monitoring must be applied to the account.



Gibraltar Financial Intelligence Unit
HM Government of Gibraltar