BAILIWICK OF GUERNSEY
LAW ENFORCEMENT

Financial Intelligence Service

Annual Report 2016

CONTACT DETAILS

ADDRESS:	Ozanne Hall Mignot Plateau Cornet Street St Peter Port Guernsey GY1 1LF
EMAIL:	fiu@gba.gov.gg
TELEPHONE:	+44 (0)1481 714081
FAX:	+44 (0)1481 710466
WEBSITE:	www.guernseyfiu.gov.gg

Guernsey Financial Intelligence Service
Annual Report 2016

MESSAGE FROM THE SENIOR INVESTIGATION OFFICER OF THE FINANCIAL INTELLIGENCE SERVICE

I am pleased to present the 2016 Bailiwick of Guernsey, Financial Intelligence Service (FIS) Annual Report. This report highlights the activity of the FIS during the year including trends, typologies, and statistics; the headline statistic being the highest ever reported number of Suspicious Activity Reports (SARs) received by the FIS. The FIS continues to proactively identify and target those engaged in financial and economic crime and terrorist financing, ensuring that the Bailiwick remains safe and secure.

In 2016, the FIS saw an increase of 40% on the number of SARs received compared to 2015 with a total of 1368 received. This is the highest figure since the FIS was formed in 2001. The continued guidance, typologies and presentations by the FIS, in conjunction with an enhanced understanding of the obligations to report is attributed to the increase in the reporting to the FIS, together with a number of international tax amnesties in place during 2016.

Strategic analysis, including identifying and evaluating the SAR data that is received, plays a pivotal role in identifying trends associated to money laundering, criminal conduct and terrorist financing. Strategic analysis also identifies the threats and vulnerabilities that could undermine the integrity and stability of the financial sector within the Bailiwick.

The top three reporting sectors for 2016 were trust and company service providers (TCSPs), banks and e-casinos. The criminality most commonly reported in SARs during 2016 was tax evasion followed by fraud, false accounting or forgery. This has been a shift from the 5 year average, where fraud, false accounting or forgery has been the reported suspected criminality of just under a third of all SARs received, followed closely by tax evasion. There has been a marked increase in SARs related to charities and non-profit organisations (NPO), although analysis reveals that a quarter of these relate to the charities/ NPOs being a victim of criminality, which has predominantly been fraud.

A main goal of the European Union's Fourth AML Directive is to prevent financial systems from being used for money laundering and terrorist financing purposes. Whilst the reporting of SARs relating to terrorist financing is relatively low in the Bailiwick (total of 8 in 2016), industry must continue to focus on preventing the movement of funds and identify terrorist financing and disrupt sources of revenue for terrorist organisations.

The FIS has previously published guidance on the reporting of 'Attempted Transactions and Activities'. There is an obligation under the Financial Action Task Force (FATF) international standards on combating money laundering and the financing of terrorism and proliferation to report suspicious transactions including 'attempted transactions'. 2016 has seen a decrease in the level of reported attempted transactions and activity to the FIS. I would encourage the reporting of 'attempts' if there is sufficient information which may identify the person(s) undertaking these 'acts'.

Cyber related crime is growing fast and evolving at a pace, becoming more aggressive and technically proficient. It is therefore a major and growing threat to the financial sector, businesses and members of the public within the Bailiwick. Guidance on cyber related crime is included in this report.

The continued hard work and dedication of my team, in conjunction with other law enforcement agencies, industry and other key stakeholders will continue to identify and target those engaged in financial and economic crime and terrorist financing.

Adrian Hale
Senior Investigation Officer, Financial Intelligence Service

THE FINANCIAL INTELLIGENCE SERVICE

The Financial Intelligence Service (FIS) is a part of the Economic Crime Division of the Guernsey Border Agency (GBA), and is Guernsey's Financial Intelligence Unit (FIU). It is jointly staffed by officers from Guernsey Police and the Guernsey Border Agency (GBA).

FIS OBJECTIVES

1. To support the work of other financial and economic crime teams, through the development of financial crime intelligence into viable financial and economic crime investigations, with an emphasis on identifying money laundering cases and the prevention and disruption of the financing of terrorism.

2. The receipt, development, analysis and dissemination of financial intelligence in a timely and effective manner and providing good quality financial intelligence to other competent authorities both domestically and internationally.

3. To maintain the security of the FIU, ensuring that the information is managed and disseminated securely and that the protection of the confidentiality of the information is maintained appropriately.

4. To respond to international requests for assistance in a timely manner, adding value where possible.

5. To facilitate the collection of SAR data through the online computer system (THEMIS) and the effective management and timely response to consent requests.

6. To provide feedback and guidance to industry to maintain the appropriateness and quality of SAR reporting.

GUERNSEY FIS AT A GLANCE

The FIS has operational independence and is free from undue influence or interference whether from political, government, industry or other sources.

OUR ROLE

'The FIS is the competent authority within the Bailiwick of Guernsey for the collection of SARs, the analysis and dissemination of financial intelligence to combat money laundering and countering the financing of terrorism'

STRATEGIC AIMS

- ◊ 'The FIS will manage the delivery of full international cooperation, within the law, to competent and relevant overseas authorities'
- ◊ 'The FIS will provide quality intelligence with regards to all aspects of financial crime investigations, with emphasis on combatting money laundering and countering the financing of terrorism, and will ensure that parallel financial investigations are undertaken in acquisitive criminal investigations'
- ◊ 'The FIS will deliver services to enhance the coordination and the development of criminal intelligence to combat financial crime'

2016 HIGHLIGHTS

40% increase in the number of SARs received on 2015

Seminar held & FIS bulletins on terrorist financing published via THEMIS to industry

31 Egmont 'requests for information' received, & 40 Egmont 'requests for information' disseminated

Effective collaborative working between FIS and other overseas authorities

Presentations delivered in Alderney, London and Oman on AML/CFT and SARs

27 Regulation 2 letters & 24 Regulation 2A letters issued

1076 disseminations made by the FIS to other competent authorities

LEGISLATION—DISCLOSURE LAW

THE DISCLOSURE (BAILIWICK OF GUERNSEY) LAW, 2007

The legal basis for the reporting of suspicion in respect of money laundering is set out in the Disclosure Law (sections 1, 2 and 3):-

- **Section 1** – Failure to disclose knowledge or suspicion etc. of money laundering – financial services businesses
- **Section 2** - Failure to disclose knowledge or suspicion etc. of money laundering – nominated officers in financial services businesses
- **Section 3** - Failure to disclose knowledge or suspicion etc. of money laundering – non financial services businesses

The legislation imposes a positive obligation to report suspicion that another person is engaged in money laundering or that certain property is or is derived from the proceeds of criminal conduct (The Disclosure (Bailiwick of Guernsey) (Amendment) Ordinance, 2014).

THE DISCLOSURE (BAILIWICK OF GUERNSEY) REGULATIONS, 2007

The Disclosure Regulations (Regulation 1) prescribes the form and manner in which disclosures are made to the FIS as the service for the receipt, analysis and dissemination of SARs within the Bailiwick and elsewhere. The online reporting facility, THEMIS, is the prescribed manner in which SARs should be reported.

REGULATION 2—ADDITIONAL INFORMATION

Obtaining additional information from reporting entities is prescribed under Regulation 2 '*Request for additional information*' which requires any person that has submitted a SAR pursuant to sections 1 to 3 of the Disclosure Law to provide the FIS with additional information.
The Regulations also provide that after a disclosure has been made, the FIS can request additional information from '***the initial disclosure***' within a specified time period (7 days), and creates an offence if this information is not provided. However, the additional material must be information which is reasonably necessary to inform a decision as to whether or not to pursue a criminal investigation.

THE DISCLOSURE (BAILIWICK OF GUERNSEY) (AMENDMENT) REGULATIONS 2014—REGULATION 2A

The Home Department introduced statutory instrument 2014/No 50 (The Disclosure (Bailiwick of Guernsey) (Amendment) Regulations, 2014) on 7th August 2014 which amended the Regulations to request additional information from third parties. This amendment extends the power to obtain additional information from any third party associated with the initial disclosure.

In accordance with Regulation 2A if an officer has reasonable cause to believe that a third party is in possession of relevant information they may request that person or entity to produce the information. The officer must confirm that this information is necessary in order to establish:

- Whether any person is engaged in money laundering; or
- That certain property is or is derived from the proceeds of criminal conduct.

THE TERRORISM AND CRIME (BAILIWICK OF GUERNSEY) LAW, 2002

The legal basis for the reporting of suspicion in respect of terrorist financing is set out in the Terrorism Law (sections 12, 15 and 15C):-

◊ Section 12 – Disclosure of information: duty of persons not connected with Financial Services Businesses;

◊ Section 15 and 15C - Failure to disclose: Financial Services Businesses.

The laundering offences created by this law are similar to the Disclosure Law, but relate to funds derived from, or likely to be used for acts of terrorism. The law also makes it an offence to fail to disclose suspicion that a person is involved in terrorist financing or laundering terrorist funds, or to tip off any person that a disclosure has been or will be made, or to provide information to any person that might prejudice an investigation.

THE TERRORISM AND CRIME (BAILIWICK OF GUERNSEY) (AMENDMENT) ORDINANCE, 2014

The May 2014 Ordinance made changes to 'Purposes of Terrorism: Interpretation'. In this Law 'purposes of terrorism' includes the provision of support to a person involved in terrorism whether or not such support is provided in relation to a specific act of terrorism. The ordinance extended the powers of the legislation to make it an obligation, under the law, to disclose knowledge, suspicion, etc. that another person is engaged in terrorist financing or suspicion that certain property is or is derived from terrorist property.

THE TERRORISM AND CRIME (BAILIWICK OF GUERNSEY) REGULATIONS, 2007

The Terrorism Regulations prescribe the form and manner in which disclosures under sections 12, 15 and 15C are made to the FIS. The online reporting facility THEMIS is the prescribed manner in which SARs should be reported under these regulations.

THE TERRORISM AND CRIME (BAILIWICK OF GUERNSEY) (AMENDMENT) REGULATIONS 2014 - REGULATION 2A

The Home Department introduced statutory instrument 2014/No 51 the Terrorism and Crime (Bailiwick of Guernsey) (Amendment) Regulations, 2014) on 7th August 2014 which amended the Regulations to request additional information from third parties. This amendment extends the power to obtain additional information from any third party associated with the initial disclosure supplied under the terrorism legislation.

In accordance with Regulation 2A if an officer has reasonable cause to believe that a third party is in possession of relevant information they may request that person or entity to produce the information. The officer must confirm that this information is necessary in order to establish;

◊ Whether any person is engaged in terrorist financing, or

◊ That certain property is or is derived from terrorist property.

LEGISLATION—PROCEEDS OF CRIME LAW

Although there is information on what is meant by the proceeds of crime available on the websites of the Guernsey Financial Services Commission and the Alderney Gambling Control Commission, institutions are reminded that under section 1 (1) of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 all offences that are indictable under the law of the Bailiwick are considered to be predicate offences, and therefore funds obtained by committing a predicate offence are considered to be the proceeds of crime.

Under Bailiwick law all offences are indictable except for some minor offences, which mainly concern public order and road traffic. Therefore, the range of predicate offences is extremely wide and includes the following:

- Participation in an organised criminal group and racketeering
- Terrorism, including terrorist financing
- Trafficking in human beings and migrant smuggling
- Sexual exploitation, including sexual exploitation of children
- Illicit trafficking in narcotic drugs and psychotropic substances
- Illicit arms trafficking
- Illicit trafficking in stolen and other goods
- Corruption and bribery
- Fraud
- Counterfeiting currency
- Counterfeiting and piracy of products
- Environmental crime
- Murder, grievous bodily injury
- Kidnapping, illegal restraint and hostage-taking
- Robbery or theft
- Smuggling
- Extortion
- Forgery
- Piracy
- Insider trading and market manipulation

INTERNATIONAL OBLIGATIONS

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the ministers of its member jurisdictions. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combatting money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is therefore a 'policy-making body' which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

The FATF has developed a series of Recommendations that are recognised as the international standard for combatting money laundering and the financing of terrorism and proliferation of weapons of mass destruction. They form the basis for a coordinated response to these threats to the integrity of the financial system and help ensure a level playing field.[1]

The FIS is required to demonstrate compliance with these Recommendations, and these Recommendations formed the basis for the MONEYVAL evaluation, against which the FIS were evaluated in 2014, and the MONEYVAL report published in January 2016.

During 2016, following analysis of the MONEYVAL report, the Bailiwick of Guernsey established an evaluation steering group to consider how to strengthen the anti-money laundering and combatting the funding of terrorism preventive measures, to which its financial institutions are subject. The following areas of enhancement are being reviewed and agreed remedial work being undertaken:

- A high level of priority and focus in respect of money laundering investigations and prosecutions.
- National Risk Assessment.
- The introduction of parallel financial investigations.
- Legislative changes.
- The production of the FIS Annual Report.

Work in these areas continues during 2017.

The full MONEYVAL report can be found here: http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/round4/GUE_MER_(2016)18_en.pdf

In July 2016, the FATF reported to the G20 on its ongoing work to tackle terrorist financing, including the effective implementation of measures to criminalise terrorist financing and freeze terrorists' assets. The FATF continues its work to strengthen the understanding of the terrorist financing threats, maintaining up-to-date and effective tools to identify and disrupt terrorist financing, and ensure that the countries are effectively implementing these tools.

The Plenary meeting of the FATF took place in Paris in October 2016. Work on terrorist financing remains the top priority for the FATF.

During this Plenary meeting, the first forum of the Heads of FIUs took place, which explored both the challenges and the best practices in obtaining beneficial ownership information, and the role of FIUs in information sharing for counter-terrorist financing purposes.

The FIS plays an important role in efforts to combat money laundering and terrorist financing; analysing suspicious transaction reports submitted by financial institutions and reporting new trends and methods that criminals use to launder the proceeds of their crime and terrorists use to raise and move their funds.

Further information about the FATF can be found here: www.fatf-gafi.org

[1] FATF-GAFI ' Who we are' (fatf-gafi.org/about/)

NATIONAL RISK ASSESSMENT

The Bailiwick of Guernsey commenced a National Risk Assessment (NRA) in 2016.

The NRA initiative concerns the assessment of the money laundering and terrorist financing risks in the Bailiwick. This initiative involves input from reporting entities and NPOs, and comprises a key part of the measures taken by the Bailiwick to meet the standards of the Financial Action Task Force (FATF) on money laundering and terrorist financing (Recommendation 1) which require each jurisdiction to identify and assess its money laundering and terrorist financing risks.

With the support of the AML/CFT authorities, the Policy & Resources Committee has liaised with the International Monetary Fund (IMF), and the authorities will be using the IMF's methodology to guide the work on Guernsey's NRA. This methodology does not replace a jurisdiction's activities in relation to risk, rather it seeks to enhance those activities and provide a skeleton based on the FATF's expectations for jurisdictions to achieve the best NRA possible.

From the FATF's perspective, money laundering and terrorist financing risks are a function of three factors: threat, vulnerability and consequence. These factors are characterised as follows by FATF guidance:

- A threat is a person or group of people, object or activity with the potential to cause harm to, for example, the state, society, the economy etc. In the money laundering/ terrorist financing context this includes criminals, terrorist groups and their facilitators, their funds, as well as past, present and future money laundering or terrorist financing activities. Threat typically serves as an essential starting point in developing an understanding of money laundering and terrorist financing risk. For this reason, having an understanding of the environment in which predicate offences are committed and proceeds of crime are generated to identify their nature (and if possible the size or volume) is important.
- The concept of vulnerabilities as used in risk assessment comprises those things that can be exploited by the threat or that may support or facilitate its activities. In the money laundering/terrorist financing risk assessment context, looking at vulnerabilities as distinct from threat means focussing on, for example, the factors that represent weaknesses in AML/CFT systems or controls or certain features of a jurisdiction. They may also include the features of a particular sector, a financial product or type of service that make them attractive for money laundering or terrorist financing purposes.
- Consequence refers to the impact or harm that money laundering or terrorist financing may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally. The consequence of money laundering or terrorist financing may be short or long term in nature and also relate to populations, specific communities, the business environment, or national or international interests, as well as the reputation and attractiveness of a jurisdiction's financial sector.

The FATF sees a NRA as the fundamental driver of a jurisdiction's approach to AML/CFT. Jurisdictions should apply a risk-based approach to allocating resources and implementing measures to prevent or mitigate money laundering and terrorist financing based on their understanding of risk as articulated in the NRA. This means that individual authorities and the authorities of a jurisdiction acting as a whole should use the NRA to prioritise their use of resources and the activities they undertake.

NATIONAL RISK ASSESSMENT

The assessment of risks in a NRA cascades through to reporting entities. In fact, this is a consequence of the risk based approach for jurisdictions embodied in a NRA. For example, jurisdictions may only permit reporting entities to take simplified measures to manage and mitigate risks if lower risks have been identified, and the standards specified below are met by reporting entities.

Reporting entities should be required to take appropriate steps to identify, assess, and understand their money laundering/terrorist financing risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). This includes being required to:

- ◊ document their risk assessments;
- ◊ consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;
- ◊ keep these assessments up to date; and
- ◊ have appropriate mechanisms to provide risk assessment information to competent authorities and Self-Regulating Bodies (SRB).

In addition, reporting entities should be required to:

- ◊ have policies, controls and procedures, which are approved by senior management, to enable them to manage and mitigate the risks that have been identified (either by the jurisdiction or by the reporting entity);
- ◊ monitor the implementation of those controls and to enhance them if necessary; and
- ◊ take enhanced measures to manage and mitigate the risks where higher risks are identified.

Clearly, therefore, an NRA will inform consideration and implementation by reporting entities of their own AML/CFT frameworks.

Several of the authorities have received substantial information from reporting entities, NPOs and other sources for a substantial period of time. We have prepared and retain comprehensive statistics and the analysis of these statistics. For many years we have articulated views on risk, based on this information.

Nevertheless, this combined information, while impressive in the context of the previous FATF Recommendations which were the subject of the MONEYVAL evaluation report on Guernsey published recently, needs to take account of the language of the current FATF Recommendations, methodology and guidance and recently published NRAs of other jurisdictions.

Guernsey's business model of cross-border customers combined with the learning which will take place internationally in relation to NRAs over the coming years suggests that our NRA will need to be particularly rigorous to be both useful and also to meet international scrutiny satisfactorily.

The Bailiwick will be continuing the NRA throughout 2017.

Further information:
www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%02013.pdf

NATIONAL RISK ASSESSMENT

The authorities, with input from the IMF, will address each of the three elements of risk (threat, vulnerability and consequence) in turn. Reporting entities and NPOs possess valuable information which will be of significant benefit for the authorities in completing the NRA.

Therefore, during June 2016, a selection of more than 60 reporting entities and NPOs were requested to complete threat perception surveys as part of the NRA process. The entities selected represented a good cross section of the types of business in the Bailiwick and international NPO activity funded in the Bailiwick. The completed surveys have not been seen by the authorities in Guernsey and the authorities will not be aware of the contents of responses made by individual entities; they will be seen only by the IMF. It is patterns of results rather than individual responses which will be particularly useful for the NRA.

The survey responses will allow the IMF to provide aggregated data to the authorities. It should also be noted that the authorities themselves and chosen counterparts in other jurisdictions have also completed surveys.

Surveys on money laundering and terrorist financing vulnerability were issued to selected entities (and authorities in other jurisdictions) prior to the workshop which was held in November 2016. Following the workshop the work on the threat and vulnerability elements of the NRA will be refined, allowing a second workshop with the IMF to be held in 2017.

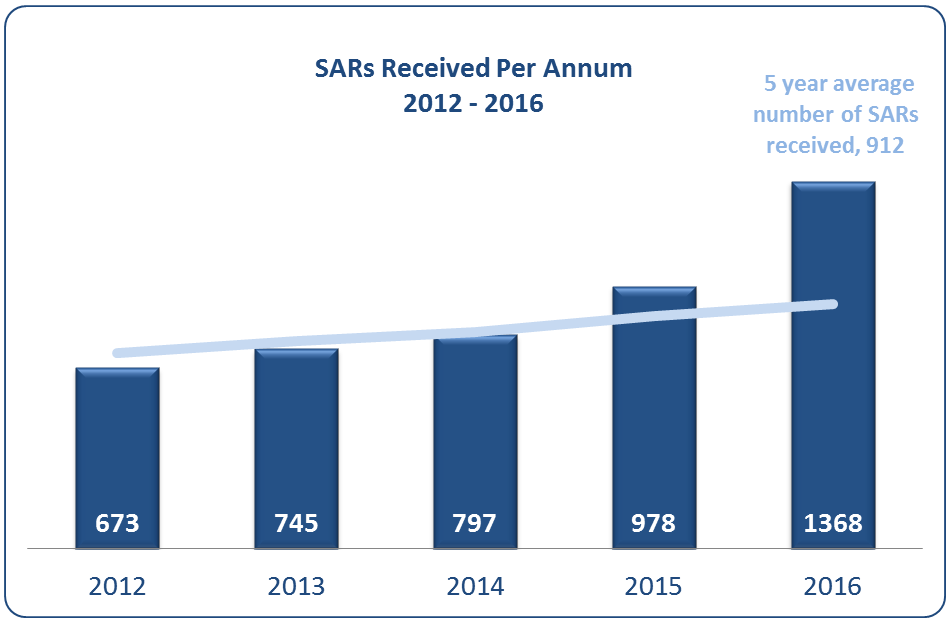
Following the completion of the NRA, assessments will need to be kept up to date. Ongoing work related to risk will be carried out after the NRA is completed, and therefore, the NRA will in practice be updated by this process. In addition, it will be necessary to revisit the NRA process itself, or elements of the process, every few years or when there are trigger events.

FATF Guidance on the NRA is available here:
www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf

STATISTICS: SARs – LEGISLATION

The FIS is the competent authority for receiving reports of suspicion or SARs, the analysis of these reports, and disseminating the results of that analysis. Analysis is carried out at both an operational and a strategic level. In addition, the FIS responds to requests for assistance from other domestic and international authorities.

The primary objective of the FIS is to receive, develop and disseminate financial intelligence in association with other agencies, in order to combat money laundering and terrorist financing, both locally and internationally. The FIS is able to obtain additional information from reporting entities and third parties and has access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.



The FIS is continuing to see an increase in the level of SARs reported. In 2016, 1368 SARs were received, representing an increase of almost 40% on 2015.

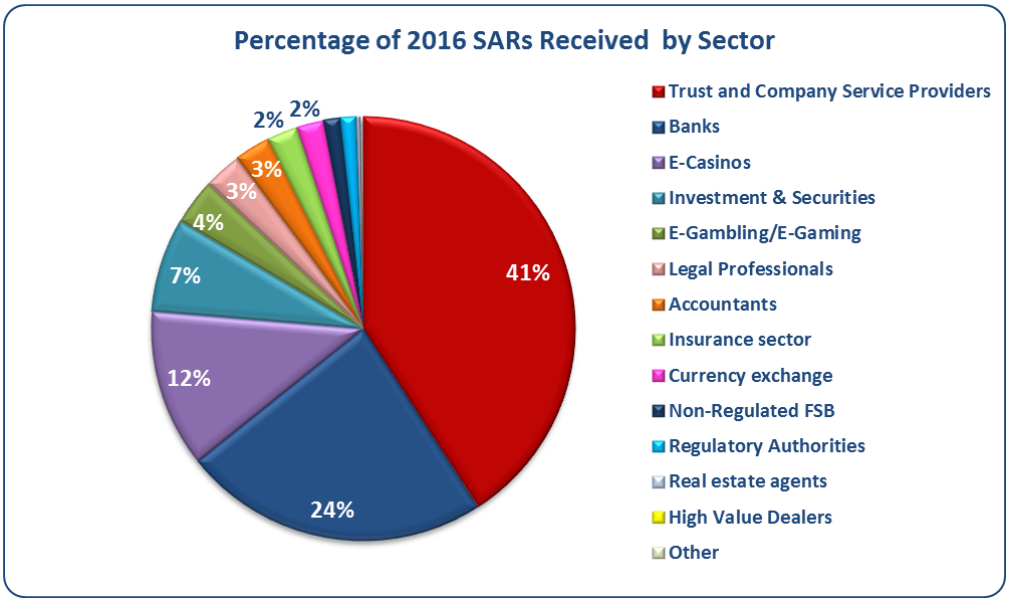
There has been a 114% increase in the volume of SARs received from e-casinos, with over half of these SARs reporting a suspicion of money laundering and 40% reporting a suspicion of fraud. The majority of these relate to due diligence issues experienced.

Efforts were made in 2016 to engage with the e-gaming sectors, and this increased awareness of reporting obligations which may have impacted on the reporting figures from this sector.

SARs RECEIVED BY LEGISLATION	2012	2013	2014	2015	2016
The Terrorism & Crime (BoG) Law, 2002	2	5	4	3	8
The Disclosure (BoG) Law, 2007	671	740	793	975	1360

Analysis of all SARs received are undertaken by the FIS, and where it is deemed to be of benefit, intelligence reports were disseminated to various competent authorities both locally and internationally.

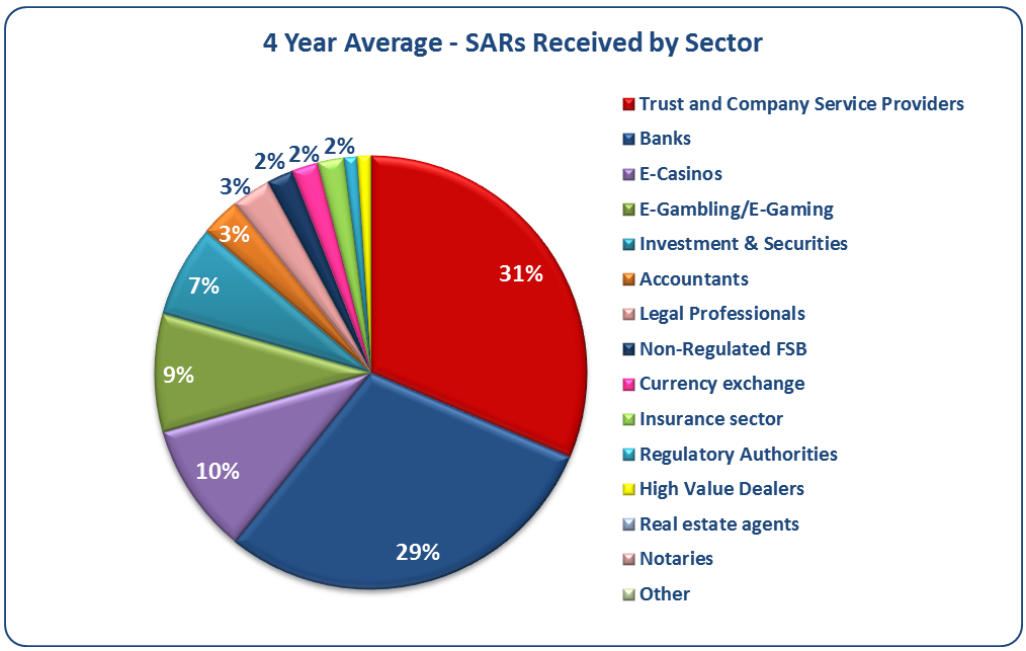
STATISTICS: SARs – SECTOR



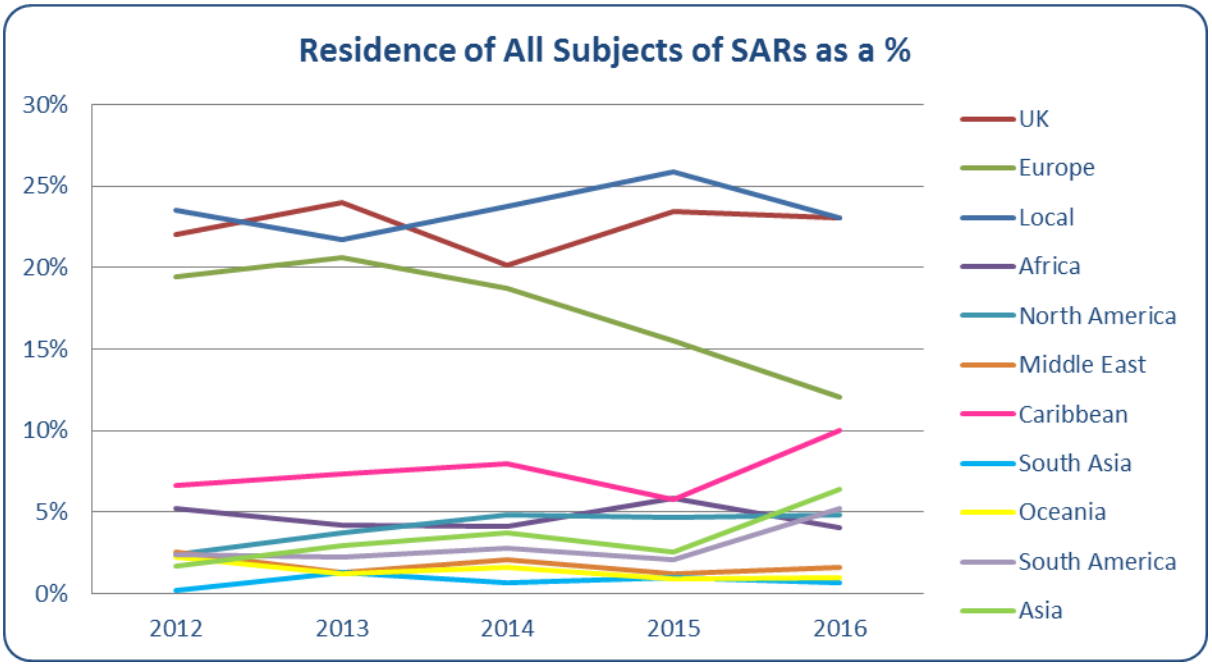
In 2016, over 40% of SARs were received from the trust and company service providers (TCSPs), followed by banks at almost 25%. This is a change from 2015, where banks submitted the greatest proportion of SARs. This may be in part due to international tax amnesties active in 2016 where clients have chosen to participate or have indicated that they will not be participating.

One TCSP entity submitted approximately 11% of all tax evasion SARs received from the TCSP sector in 2016, the majority of which were linked to an international tax amnesty.

The top three reporting sectors by number of SAR submissions in 2016 (trust and company service providers, banks, and e-casinos) are also mirrored in the four year average number of SARs received by sector, which reflects that nature of business undertaken in the Bailiwick.



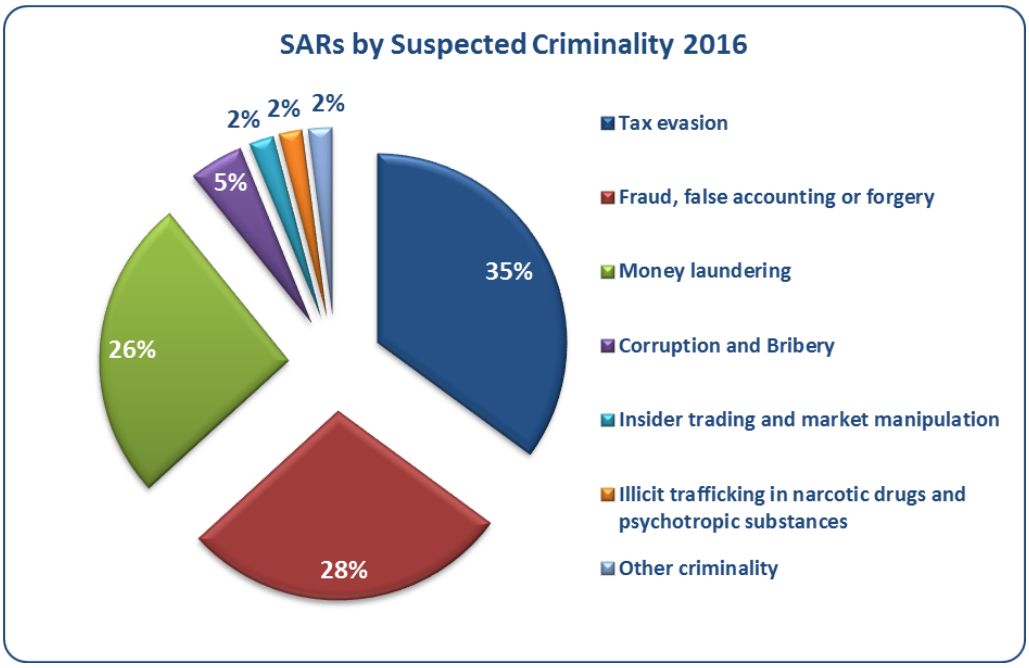
STATISTICS: SARs – RESIDENCY



Most subjects of SARs reside locally or in the UK.

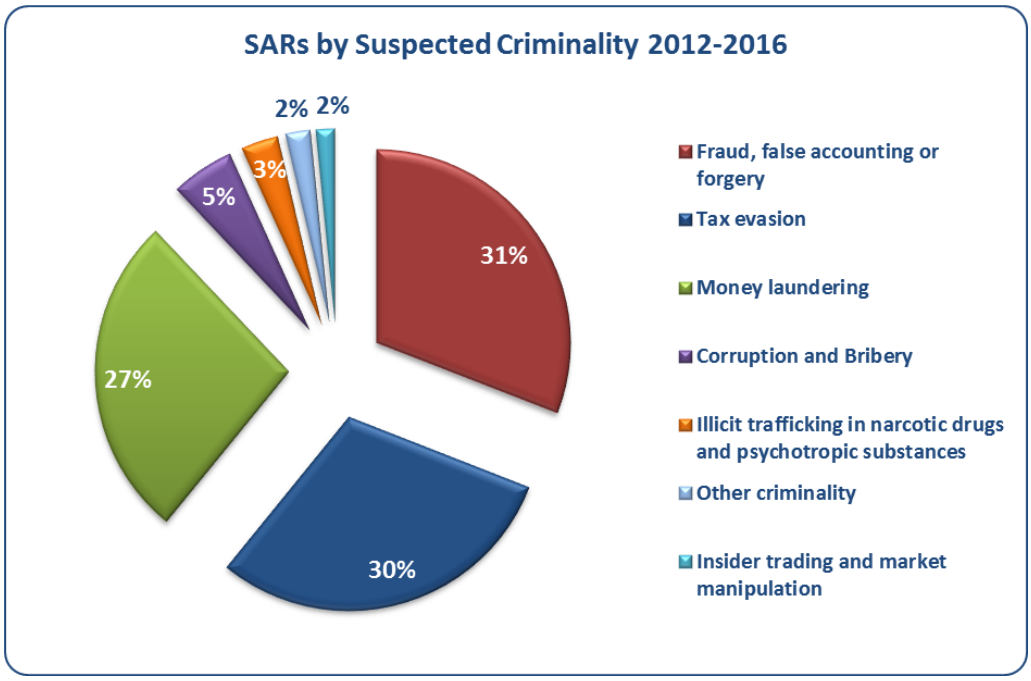
There has been a continuing decline in SARs related to Europe based entities, which may be due to the changing nature of jurisdictions where business is established.

STATISTICS: SARs – SUSPECTED CRIMINALITY

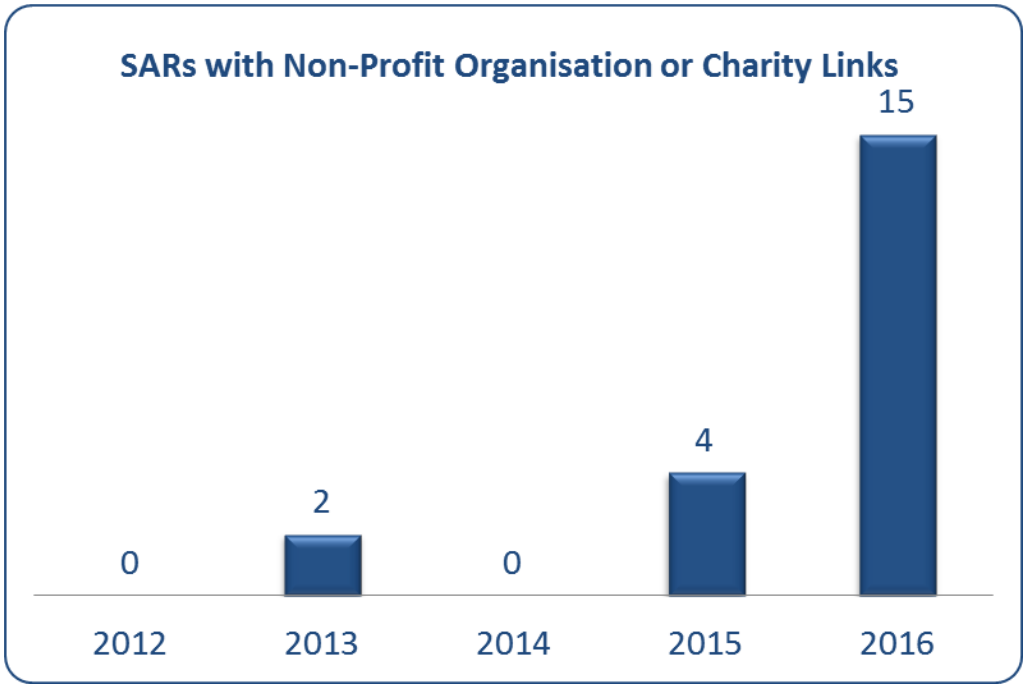


In 2016, tax evasion was the predominant criminality reported, followed by fraud, false accounting or forgery, which differs from the five year trend of fraud, false accounting or forgery being the most reported suspected criminality. The reason for tax evasion becoming the top reported suspected criminality is likely due to tax amnesties in place during 2016.

The four criminalities reported most frequently in the five year period 2012-2016, and also in 2016 specifically are fraud, false accounting or forgery; tax evasion; money laundering; and corruption and bribery, although the proportions of each criminality vary.

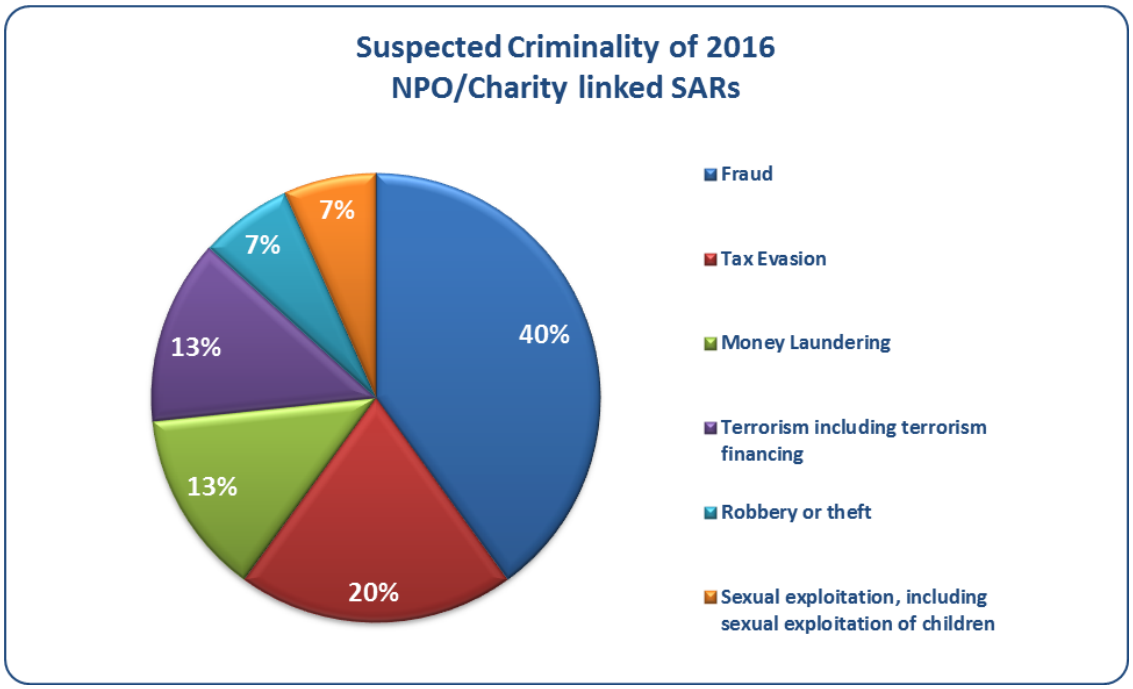


STATISTICS: SARS — NON-PROFIT ORGANISATIONS/CHARITY



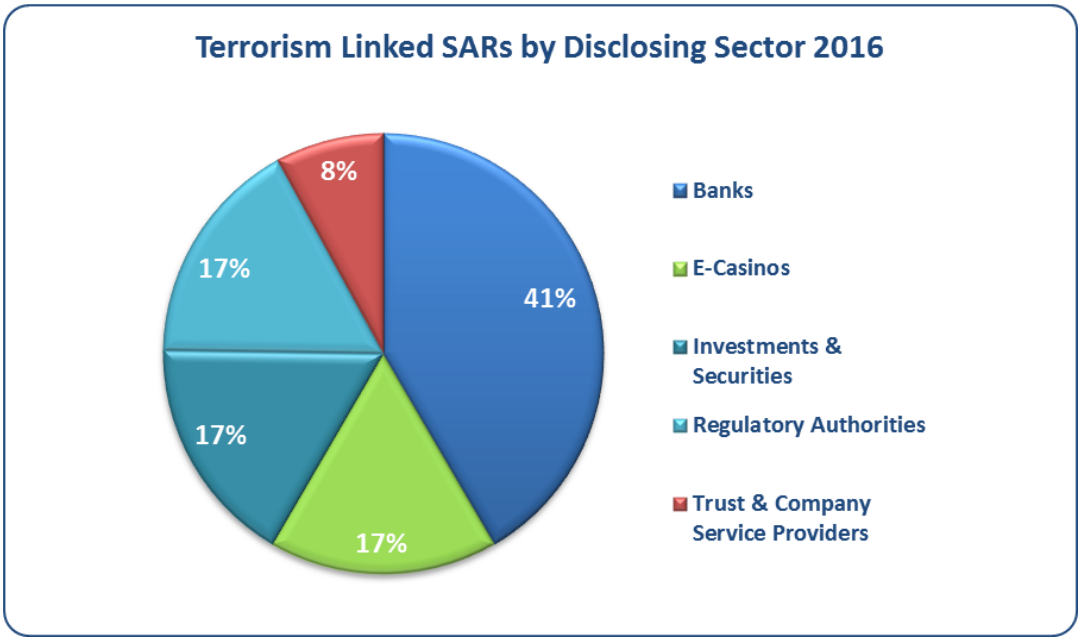
In 2016, 40% of SARs received that linked to charities or NPOs reported a suspicion of fraud. 25% of NPO/charity linked SARs relate to the charity being a victim of fraud or theft rather than a vehicle for criminality to be committed.

60% of all NPO/charity related SARs were received from the banking sector.

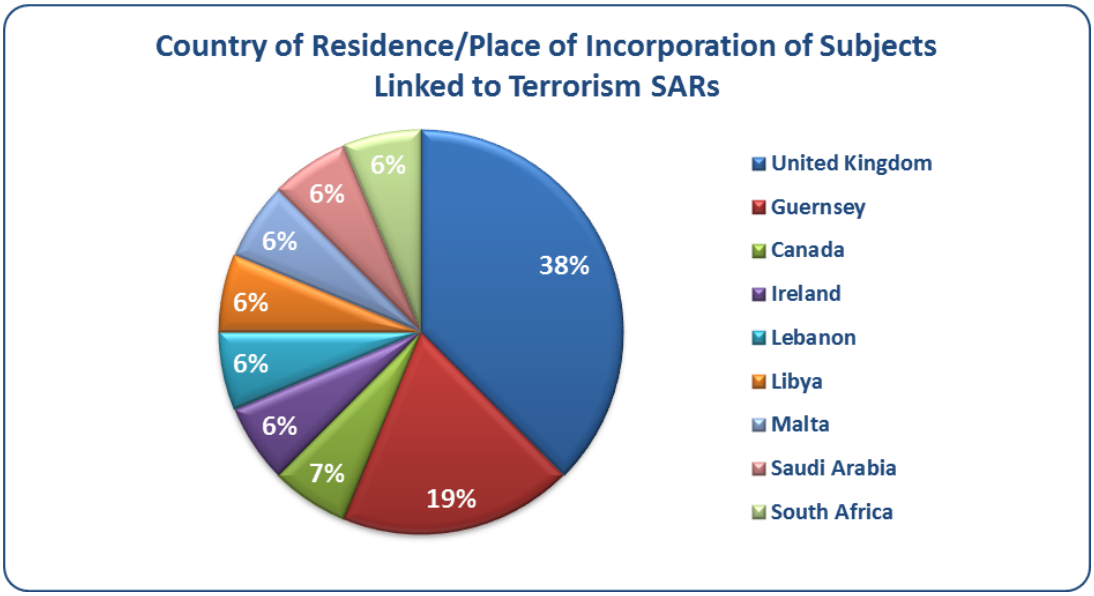


STATISTICS: SARs – TERRORISM

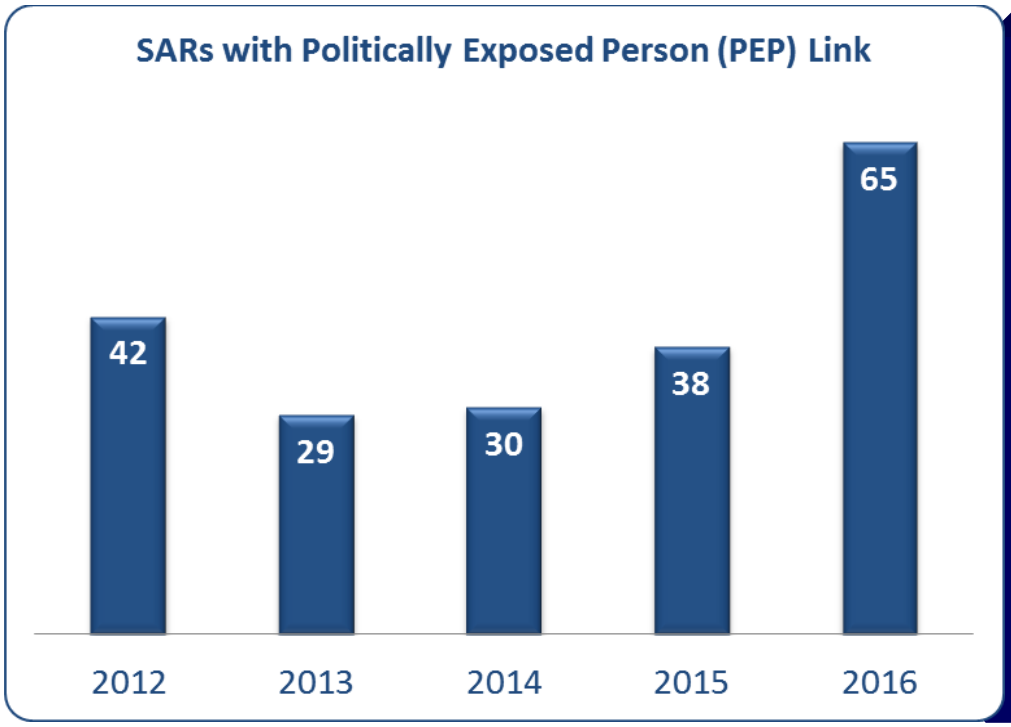
Analysis of all SARs received under the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 are undertaken by the FIS. Following analysis, in the majority of cases intelligence reports were disseminated to various competent authorities. The figures of SARs submitted in relation to terrorism remain low, and as such no clear trends have been identified.



In 2016, twelve SARs were received that contained links to terrorism. Eight of these SARs were disclosed under the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002. Four were disclosed under the Disclosure (Bailiwick of Guernsey) Law, 2007 as terrorism links were identified following FIS analysis of the SARs. Disseminations are made to the relevant competent authorities both locally and internationally if after analysis of the SAR, it is deemed appropriate to do so.



STATISTICS: SARs — PEPs

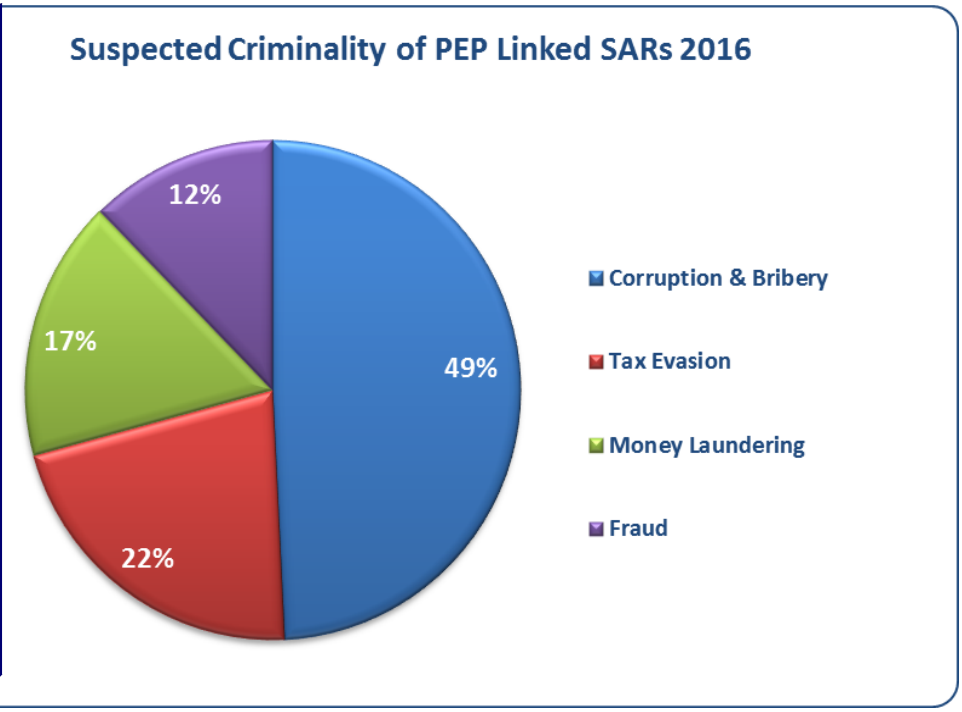


Approximately 4% of SARs over the 5 year period showed a link with a Politically Exposed Person

'Politically Exposed Person (PEP)[1]' means a natural person who is or who has been entrusted with prominent public functions.

There has been a slight increase in the number of PEP linked SARs in 2016, which is attributed to changes in the manner in which the FIS analyse the data, although the proportion of SARs with a PEP link in 2016 remains low at 5%.

Trust and company service providers submitted the highest proportion, (over 50%) of PEP linked SARs in 2016

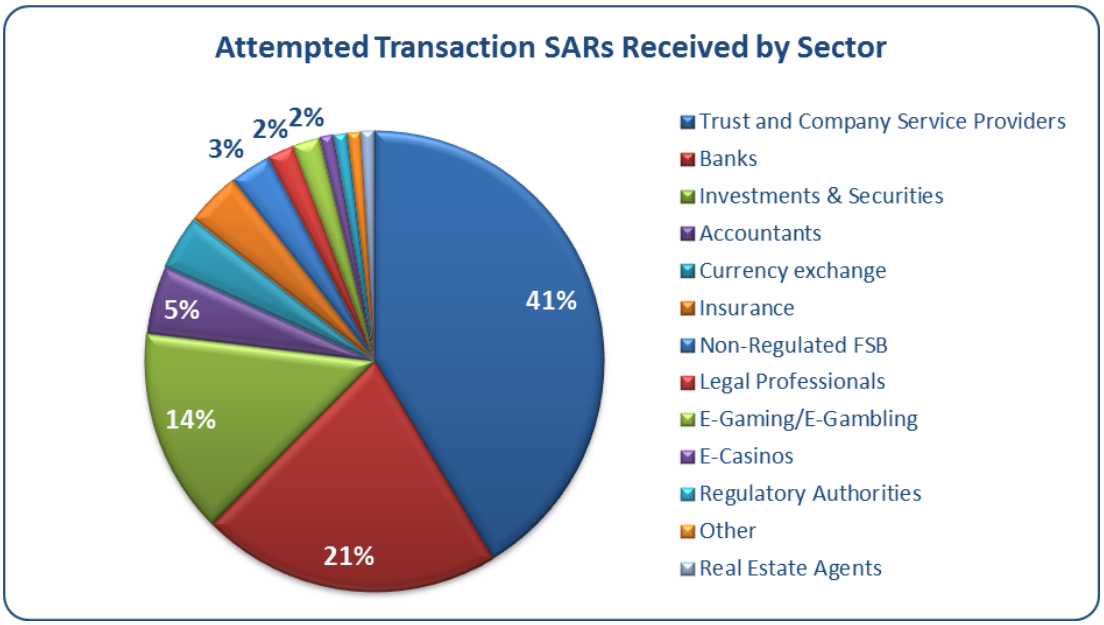


[1]*DIRECTIVE (EU) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC*

STATISTICS: SARs — ATTEMPTED TRANSACTIONS

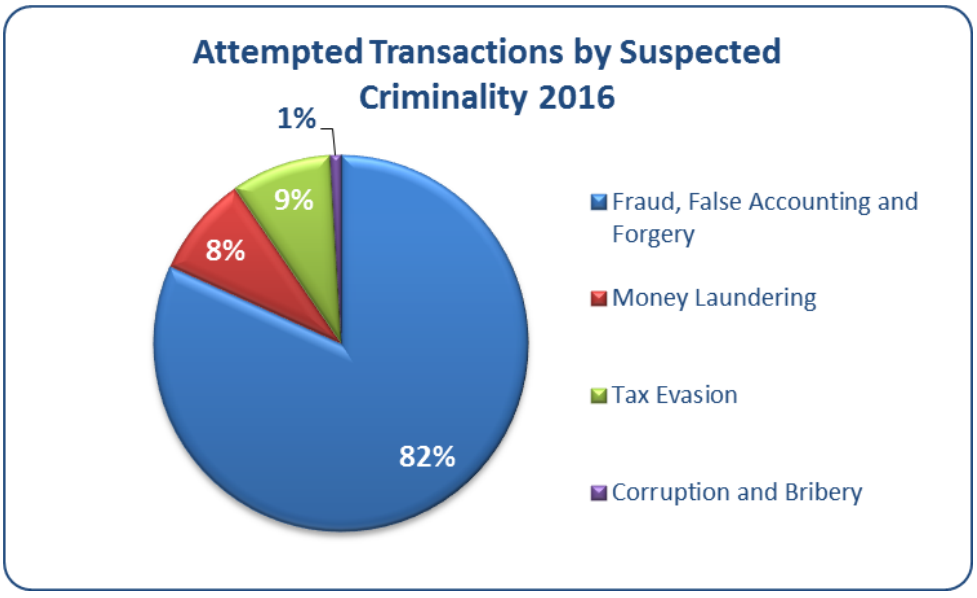
Attempted transactions have been recorded since 2013 and in 2016 they comprised approximately 8% of the annual total of SARs received; a decrease of 4% on 2015. The investments and securities sector reported a greater number of attempted transactions than in 2015, whilst banks and trust and company service providers reported fewer attempted transactions than in 2015.

The increased number of reports from investments and securities could be attributed to a greater awareness of the reporting requirements for attempted transactions.



The majority of attempted transaction reports were submitted by trust and company service providers.

Over 80% of attempted transactions received in 2016 suspected fraud, false accounting or forgery as the criminality.

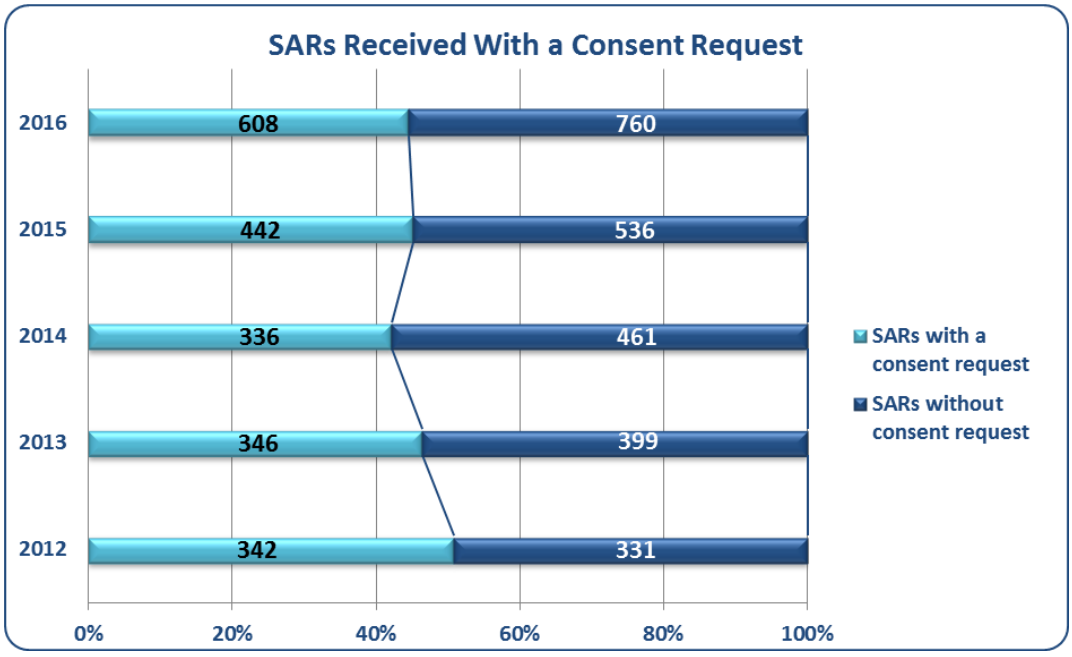


The FIS has previously issued guidance on 'attempted transactions' which can be found on the website, www.guernseyfiu.gov.gg

STATISTICS: SARS — FIS ACTION & PROVISIONAL MEASURES

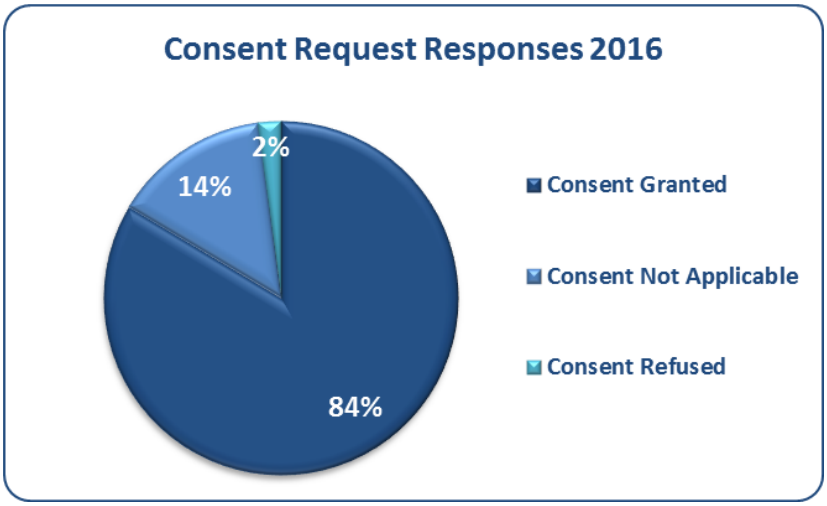
While there is no express power under Bailiwick legislation for the FIS to postpone transactions, postponement is achieved when the FIS refuses to consent to an act (transaction) following the making of a report of suspicion in respect of it. Because consent from the FIS constitutes a defence to a charge of money laundering in respect of the relevant transaction and as the service provider will not proceed with the activity for fear of committing a money laundering offence, the effect of withholding consent, in practice, prevents the transaction taking place.

In cases where consent is requested and the FIS has been unable to establish a link to criminality, consent is granted.



The graph above shows the number of SARs received with a consent request included at submission. As it is possible to request consent after submission of the SAR, each SAR may have more than one consent request attached to it.

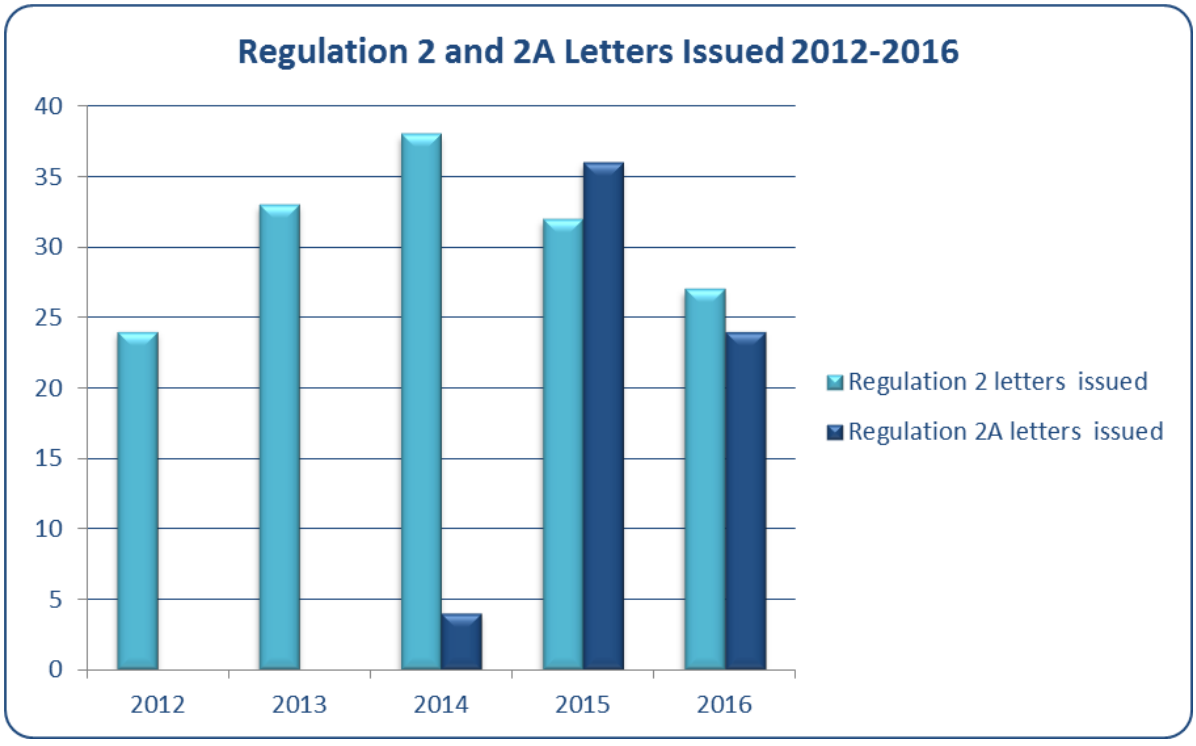
In 2016, a total of 1,018 consent requests were received by the FIS. Of these 84% were granted, 14% were considered to not be relevant consent requests and 2% were refused.



STATISTICS: SARS — REGULATION 2 & REGULATION 2A

Under Regulation 2 of the Disclosure Regulations and the Terrorism Regulations, the FIS may serve a written notice on a person who has made a SAR, requiring that person to provide such additional information relating to the SAR as may be specified. Ordinarily, the information must be provided within 7 days, but the FIS may extend the 7 day period and may also reduce it to a reasonable lesser period in urgent cases. Failure without reasonable excuse, to comply with a notice in the specified time frame is a criminal offence.

Under Regulation 2A, if a SAR has been made, the FIS can request information relating to that SAR from a third party, if it is satisfied that there are reasonable grounds to believe that the third party possesses such information, and also that there are reasonable grounds to believe that the information is necessary to the FIS for the proper discharge of its functions.



In 2016, 27 Regulation 2 letters were issued by the FIS, and a further 24 Regulation 2A letters were issued. The use of both Regulation 2 and Regulation 2A has been a vital tool in the progression of numerous investigations.

In the majority of cases, the information obtained has been disseminated as intelligence to both local and overseas authorities for further investigation.

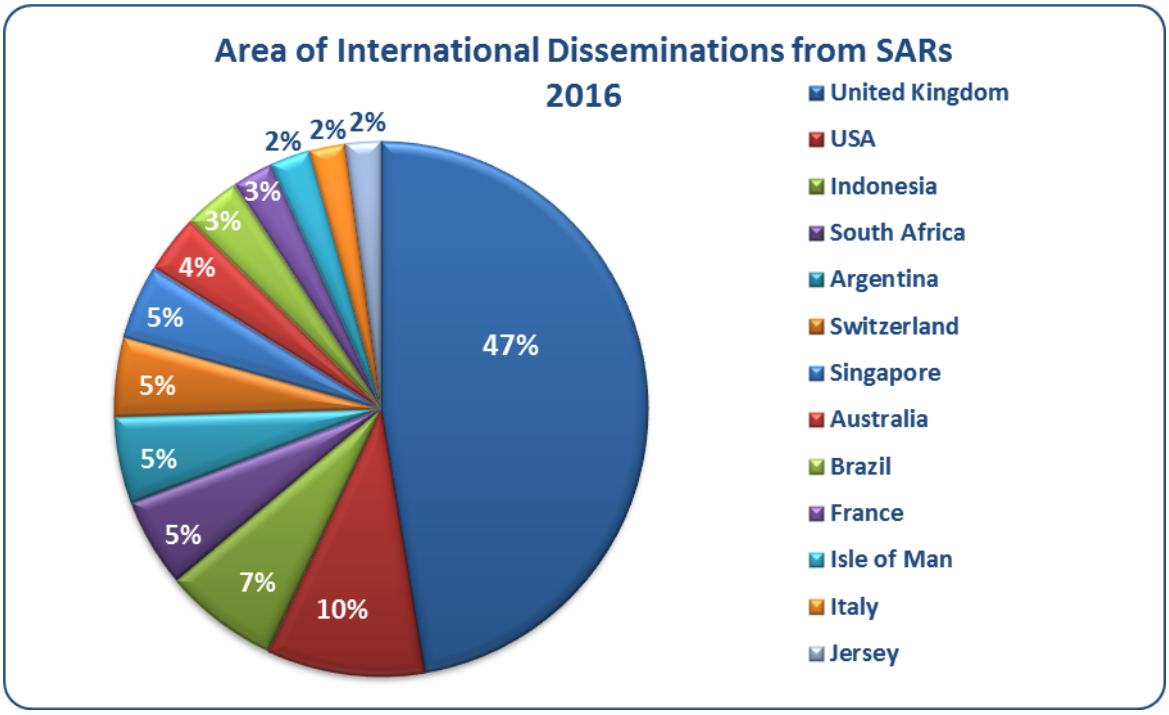
STATISTICS: SARS — DISSEMINATIONS

	2012	2013	2014	2015	2016
Total SARs received	673	745	797	978	1368
Local disseminations	93	84	90	132	208
International disseminations	390	473	520	539	868
Total number of disseminations	483	557	610	671	1076

Where relevant, intelligence received by the FIS is disseminated. In 2016, 1076 disseminations were made from the FIS. Over 80% of these disseminations were to international authorities, including the USA, Indonesia, South Africa, Argentina, and Switzerland. This indicates that the SARs refer mainly to activities abroad, which reflects the character and the nature of the financial services businesses in Guernsey.

Local disseminations accounted for almost 20% of disseminations and were made to law enforcement and to other authorities within the Bailiwick of Guernsey.

Disseminations were made during 2016 to 109 different FIUs or law enforcement agencies. The major area for dissemination was to the UK.



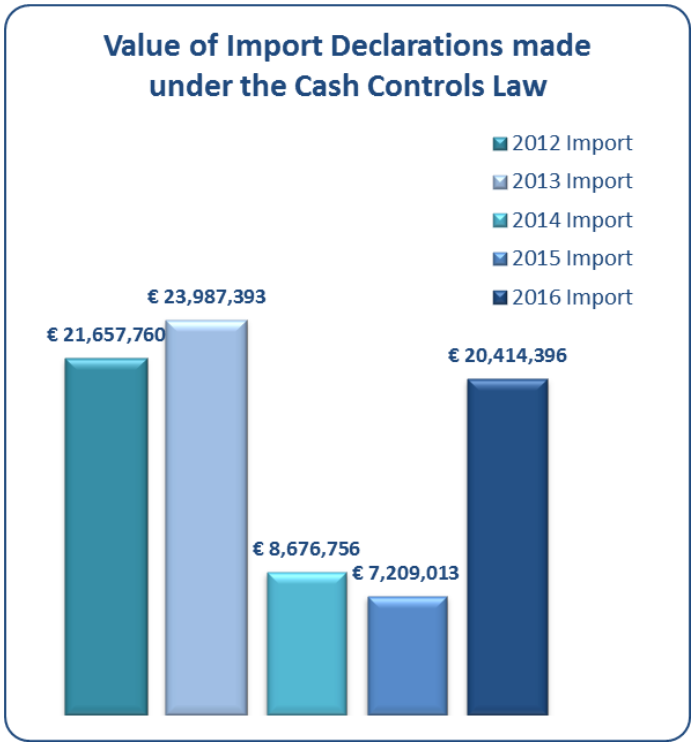
CROSS BORDER TRANSPORTATION OF CURRENCY & BEARER NEGOTIABLE INSTRUMENTS

All cross border transportation of currency must be reported, irrespective of suspicion. This is because The Cash Controls (Bailiwick of Guernsey) Law, 2007 prohibits the carrying of cash, in excess of €10,000, into or out of the Bailiwick unless it has been declared.

Cash is defined for the purposes of the Cash Controls Law as –

a) Bearer negotiable instruments including monetary instruments in bearer form, such as travellers' cheques, negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery, incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee's name omitted; and

b) Banknotes, bullion (which includes gold, silver palladium and platinum bullion whether pure or impure) ingots and coins (whether or not in circulation as a medium of exchange).



Total number of declarations and method of import and export of cash from the Bailiwick 2012-2016

	Total Declarations	Import	Export	Air Travel	Sea Port
2012	226	139	87	138	88
2013	211	133	78	131	80
2014	120	65	55	71	49
2015	116	62	54	71	45
2016	107	72	35	17	90

PARALLEL FINANCIAL INVESTIGATIONS

The FATF defines a financial investigation as 'an enquiry into the financial affairs related to a criminal activity, with a view to: (i) identifying the extent of criminal networks and/or the scale of criminality; (ii) identifying and tracing the proceeds of crime, terrorist funds or any other assets that are, or may become, subject to confiscation; and (iii) developing evidence which can be used in criminal proceedings.'

The FATF Recommendation 30 describes a parallel financial investigation as 'conducting a financial investigation alongside, or in the context of, a (traditional) criminal investigation into money laundering, terrorist financing, and/or predicate offence(s).'

This links to Immediate Outcome 7 'money laundering offences and activities are investigated and offenders are prosecuted and subject to effective, proportionate and dissuasive sanctions' where the characteristics of an effective system are stated as 'money laundering activities, and in particular major proceed-generating offences, are investigated; offenders are successfully prosecuted; and the courts apply effective, proportionate and dissuasive sanctions to those who are convicted. This includes pursuing parallel financial investigations and cases where the associated predicate offences occur outside the country, and investigating and prosecuting stand-alone money laundering offences.'

The FIS undertakes parallel financial investigations.

In 2016, the FIS disseminated fifteen cases for further investigation to local law enforcement, of which six related to parallel financial investigations. Of these cases; one resulted with an individual being sentenced to two years imprisonment for drug offences and possession of a prohibited weapon, with a confiscation order to follow in 2017.

Following analysis of a disclosure received by the FIS, where the subject was identified as a 'victim' of a suspected fraud, two Egmont requests were sent to Portugal FIU to ascertain further information which resulted in the dissemination of the intelligence to local law enforcement. This resulted in executive action being undertaken in respect of the person concerned with the fraudulent act. Charges of fraud have followed with the case ongoing.

Following a disclosure received, the FIS identified a male and female who were sending cash via special delivery to a PO Box address. When asked about the posting, they were evasive. Enquiries conducted by the FIS identified two individuals and intelligence was disseminated to local law enforcement. Executive action took place, resulting in the individuals being arrested following a controlled delivery and a quantity of pills identified within the postal system. One individual appeared in the Royal Court charged with being knowingly concerned in the importation of a Class C controlled drug, and was sentenced to three years and six months imprisonment.

The FIS assisted law enforcement with financial enquiries regarding the subject of one of their investigations. The subject of investigation appeared before the Royal Court for sentencing in 2016. The subject had been charged with a number of counts of fraud whilst working as a director at a trust and company service provider. In court the subject was sentenced to two years concurrent for all counts of fraud.

INDUSTRY OUTREACH

In 2016, the FIS delivered presentations to industry and other key stakeholders, both locally and overseas. Some of these were delivered in conjunction with other regulatory agencies, such as the Alderney Gambling Control Commission (AGCC) and the Guernsey Financial Services Commission (GFSC).

Topics presented in 2016 included:

- ◊ Financial Investigation Tools
- ◊ International Standards on the Combatting of Money Laundering and Financing of Terrorism
- ◊ Suspicious Transactions Awareness Forum
- ◊ Terrorist Financing Seminar

In June, the FIS delivered a financial awareness presentation in Alderney to private entities regarding the combatting of money laundering and the financing of terrorism. This was followed up in October by a presentation delivered in London, in conjunction with the AGCC, to the e-gaming and e-casinos sectors. These presentations provided an opportunity to continue to engage with and update these sectors on developments within the FIS and the associated reporting standards.

Similar presentations were delivered to private sector entities throughout the year.

In October, the FIS in conjunction with the GFSC delivered a terrorist financing seminar. This event was attended by 165 people and 108 firms were represented.

The FIS has continued to publish notices via the online reporting portal THEMIS, to registered entities on a variety of subjects. In 2016 the FIS published 84 notices via THEMIS including sanction notices, publications of information, email scam notifications, potential fraud notifications, and consultation papers.

The FIS are aware that notices such as sanctions may be available from other sources and thus represent a duplication of information; however, the manner of dissemination from the FIS is considered to be an efficient method to provide key AML/CFT information to a wide forum, effectively and expeditiously.

The FIS seeks feedback from entities who attended these presentations and received guidance notices as to how useful they have been in enhancing recipients understanding of their role within combatting money laundering and terrorist financing.

Feedback is requested to be sent to FIU@gba.gov.gg

The FIS publishes risk warnings to industry through the THEMIS portal, and publishes news regarding the work of the FIS on the FIU website.
Further information on Industry Outreach is available on guernseyfiu.gov.gg

INDUSTRY OUTREACH:
SUSPICIOUS TRANSACTION AWARENESS FORUM, OMAN

In November 2016, Adrian Hale the Senior Investigation Officer responsible for the FIS was invited to Oman to participate as a national expert at the Suspicious Transactions Awareness Forum at the Crowne Plaza Hotel, Muscat.

The forum was organised and funded by the National Committee for Combating Money Laundering Terrorism Financing and the National Centre for Financial Information. The opening ceremony and forum was attended by public officials, directors of government agencies, financial agencies and institutions, non-financial businesses and professions, and non-profit associations and bodies from Oman and other countries from the Arabian Peninsula.

The three day forum aimed to develop the knowledge and experience of domestic and international developments in the field of combating money laundering and terrorist financing. There were a number of presentations and working papers on key areas of AML/CFT from key speakers from Austria, Australia, Guernsey, Italy, Oman, The Netherlands, United Kingdom and United States of America.

The forum focused on the roles of a FIU, SARs, asset recovery (criminal and civil), corruption, cybercrime, beneficial ownership, correspondent banking, de-risking and international co-operation and co-ordination in the fight against money laundering and terrorist financing.

Further information on Industry Outreach is available on guernseyfiu.gov.gg

INDUSTRY OUTREACH: TERRORIST FINANCING

In 2016, the FIS provided guidance on Terrorist Financing.

In January, a bulletin was distributed to industry via THEMIS on 'Foreign Terrorist Fighters' (FTFs). This bulletin was based upon analysis following work undertaken by the Egmont Group of Financial Intelligence Units along with the Financial Action Task Force (FATF). This bulletin aimed to share key findings with appropriate reporting institutions and to raise awareness of some of the characteristics of financial transactions that may indicate terrorist financing.

In September, a second bulletin was issued by the FIS 'Detecting Terrorist Financing: Relevant Risk Indicators'. The aim of the bulletin was to help AML/CFT authorities and private sector entities to detect and disrupt the financial flows of terrorists and terrorist organisations.

These bulletins were supported by a joint seminar on terrorist financing delivered in October by law enforcement and the Guernsey Financial Services Commission to industry.

The aim of this seminar was to raise awareness of terrorist financing and how industry can assist in the detection and prevention of terrorism and terrorist financing.

Feedback provided from these publications has indicated that the material has raised awareness of terrorist financing and will be incorporated into training materials within local businesses.

As appropriate, the FIS will continue to publish bulletins related to areas of risk and of interest to industry via THEMIS.

The FIS publishes Risk Warnings to industry through the THEMIS portal, and publishes news regarding the work of the FIS on the FIU website.

INDUSTRY OUTREACH: CYBERCRIME

The FIS has provided guidance on cybercrime by way of presentations and notices issued to industry on the FIU website and via THEMIS.

The FIS has received reports of both attempted and successful transactions resulting from cyber-enabled crime, which have been conducted by way of compromised email accounts requesting a transaction or action which may or may not have been executed dependent on at what stage a suspicion was formed i.e. hacked emails used to commit crimes such as fraud.

There have been reported cases of 'spear-phishing' where targeted emails attempt to trick the recipient into sharing sensitive information such as passwords, usernames or financial details, and 'whaling' whereby an email is received by a member of staff purporting to be from an executive of the entity requesting information or a payment to be made. These attacks are personalised towards the target by making the email appear legitimate and appear as if they are sent from trusted entities.

These can originate from a hacked or 'spoofed' email account(s), or from email addresses similar to the executives email address, with some characters substituted i.e. 'rn' replaces 'm', or a '1' replaces an 'l'.

Where a transaction is requested there is often an urgency to complete the transaction and frequent email or phone contact from the fraudster, and the payment request may be unusual i.e. to an unusual jurisdiction for the client, or with companies that the client has not transacted with before.

The FIS has also seen reports of 'mandate fraud' where contact is received requesting a change to bank account details on an invoice and, if actioned, a fraud is committed. To avoid a fraud being committed, if an unusual request is received, verification steps should be taken via another channel to ensure that the person who is stated to have sent the instruction, has in fact done so.

Risks are also posed from insider threats, i.e. data theft by a contracted third party, or by employees; key logging; misuse of computers; ransomware; malware and DDOS attacks.

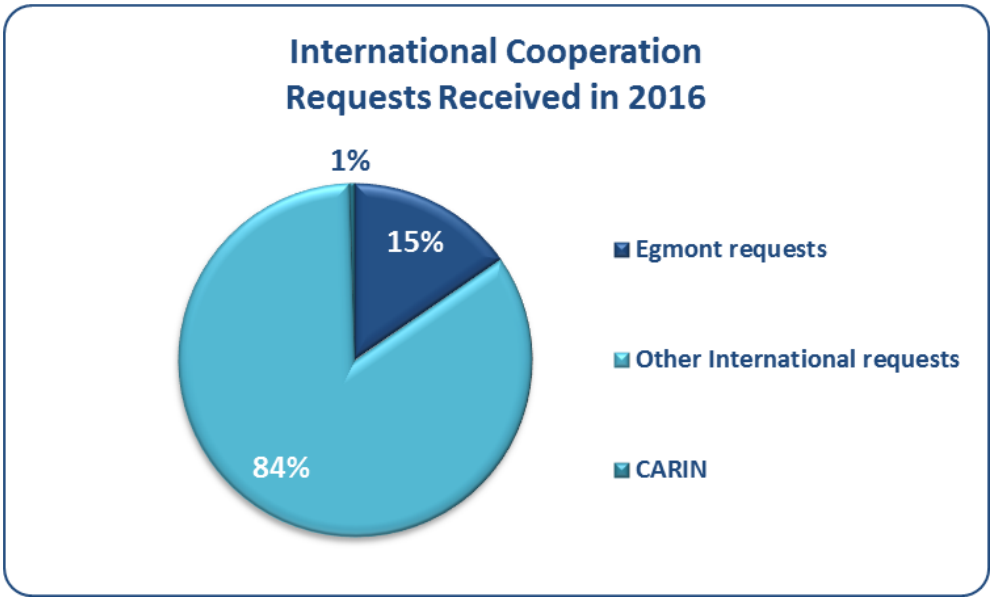
To minimise the risks from these attacks, businesses should review their own internal processes and procedures and train staff in cyber security awareness to ensure that all staff are aware of the risks associated to cyber security, and take steps to verify any requests which seem unusual.

Where a financial act has been attempted, or has been successful, a SAR can be made to the FIS via the THEMIS portal.

The FIS publishes Risk Warnings to industry through the THEMIS portal, and publishes news regarding the work of the FIS on the FIU website

INTERNATIONAL COOPERATION

The FIS exchanges information freely, spontaneously and upon request with foreign FIUs, regardless of their status. Guernsey does not require a Memorandum of Understanding in order to exchange information, which can be achieved through its existing legal framework. It will nevertheless enter into agreements if required by other jurisdictions or organisations, and has currently signed MOUs with 30 different parties.



During the early part of 2016, the FIS assisted the Bulgarian authorities with intelligence which has resulted in the forfeiture of assets to the sum of approximately 1.1 billion euros. This case commenced as a result of a meeting between the Republic of Bulgaria and Guernsey during a CARIN meeting held in EuroPol. A SAR submitted from a Guernsey institution and subsequent analysis and development work undertaken by the FIS resulted in a dissemination of the intelligence to Bulgaria. The Guernsey element of the case is ongoing with a formal mutual legal assistance request expected from Bulgaria.

Guernsey plays a significant role in international asset recovery and sharing of intelligence to other competent authorities.

In April 2016, a SAR was received, and after analysis, intelligence was disseminated to the National Crime Agency, and subsequently Norfolk police arrested and convicted the subject for fraud. The Regional Economic Crime Unit dealt with the confiscation and repatriation of the funds and contacted the FIS in Guernsey who advised them that there would be no need for a formal mutual legal assistance request as a SAR had been submitted and the FIS could consent for the payment to be made back to the victim. Subsequently, the FIS, along with the institution agreed to refund the full amount back to the victim of the crime.

Following a disclosure received by the FIS in July 2016, analysis on the SAR resulted in several disseminations of intelligence to the South African FIU. A response was received from the FIU indicating that there was a potential criminal investigation in South Africa.

These cases demonstrate some excellent examples of collaborative working between the FIS, disclosing institutions and overseas authorities.

INTERNATIONAL COOPERATION: EGMONT GROUP

In 1995, a group of FIUs decided to establish an informal group for the stimulation of international cooperation. Now known as the Egmont Group of Financial Intelligence Units, these FIUs meet regularly to find ways to cooperate, especially in the areas of information exchange, training and the sharing of expertise. Egmont provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and the financing of terrorism of which the FIS is a member.

The goal of the Egmont Group is to provide a forum for FIUs from around the world to improve cooperation in the fight against money laundering and financing of terrorism and to foster the implementation of domestic programs in this field.

As a member of the Egmont Group, the FIU is able to send requests for information to other member jurisdictions by the Egmont Secure Web (ESW) secure email network and also receive requests from other Egmont Group members.

In 2016, the FIS received 31 Egmont requests for information. These were received from jurisdictions including the UK, the Czech Republic, Liechtenstein, Bangladesh, Ukraine and the United States of America.

In 2016, the FIS received 31 Egmont requests for information

When a request for information is received by the FIS, it is acknowledged upon receipt, and responded to in a timely manner, dependent on the nature and detail of the information requested. The FIS provides full cooperation to the requesting jurisdiction.

The most frequently identified predicate offences within the received Egmont requests are money laundering, fraud and tax evasion.

In 2016, the FIS sent 40 Egmont requests for information

In 2016, the FIS sent 40 Egmont requests for information to 23 jurisdictions, including Hong Kong, Hungary, Switzerland, Slovakia, UAE, USA, and Jersey.

Intelligence shared between jurisdictions is crucial for the analysis of SARs and for the development of intelligence for dissemination. Timely responses and quality intelligence are essential for the jurisdiction to develop the intelligence .

40% of the Egmont requests sent by the FIS relate to 7 operational law enforcement cases. The information included in these requests may be used for intelligence purposes only and may only be forwarded to law enforcement with the express consent of the disseminating FIU. If the information is required for evidential purposes, law enforcement must request the information by way of submitting a mutual legal assistance request to the appropriate jurisdiction.

Information on the Egmont Group can be found here: www.egmontgroup.org/

INTERNATIONAL COOPERATION: CARIN

CARIN is a network of judicial and law enforcement expert practitioners in the field of asset identification, seizure and confiscation.

There are currently 62 countries and jurisdictions and nine international organisations that are members of the network.

All EU countries are represented in CARIN, together with non-EU jurisdictions such as the United States of America, South Africa, Australia, Canada, Russia and Switzerland, as well as Guernsey. Europol, Eurojust, OLAF, the UNODC, and the International Criminal Court are also CARIN Members.

CARIN is now recognised globally as an effective tool to fight international crime and the network now covers more than 110 countries and jurisdictions. There are also proposals to extend the network to other countries during 2017.

Early in 2016, Guernsey formally handed over the CARIN Presidency to the Netherlands who will undertake the Presidency for 2016.

The 2016 CARIN annual regions meeting took place in Rotterdam on 26th and 27th May 2016 and was attended by over 170 participants. The focus of the conference was exchanging information and improving the exchange of information between CARIN members, enhancing the registration of international confiscation including alternative ways of cross border asset management and a multidisciplinary approach to confiscation and how to improve asset recovery with all government institutions working collectively and disruption through joint agency cooperation. Guernsey law enforcement were involved in facilitating the workshop on exchange of information.

The 2017 CARIN Presidency will be undertaken by Sweden.

CARIN Meeting at Europol 2016

Further information on the CARIN Network can be found on www.carin-network.org

QUESTIONS & ANSWERS — SARS

PLEASE NOTE THAT THESE Q&As CONSTITUTE BRIEF GUIDANCE AND ARE PROVIDED FOR INFORMATION ONLY

QUESTION: What is a SAR or Disclosure?

ANSWER: A SAR is a Suspicious Activity Report or a Disclosure. A person must make a required disclosure (as soon as possible) if you know or suspect or have reasonable grounds for knowing or suspecting that another person is engaged in money laundering or that certain property is or is derived from the proceeds of criminal conduct or terrorist financing.

QUESTION: Which law should I disclose under?

ANSWER: The legal basis for the reporting of suspicion in respect of money laundering is set out in The Disclosure (Bailiwick of Guernsey) Law, 2007. The legal basis for the reporting of suspicion in respect of terrorist financing is set out in The Terrorism and Crime (Bailiwick of Guernsey) Law, 2002.

QUESTION: When should I submit a SAR (Disclosure)?

ANSWER: A person acting in the capacity of a financial services business or a non-financial services business is required to submit a SAR to a prescribed police officer who is a member of the FIS as soon as that person knows or suspects (or has reasonable grounds for knowing or suspecting) that another person is engaged in money laundering or terrorist financing or that certain property is or is derived from the proceeds of criminal conduct or terrorist financing.

Further to that the information or other matter on which the knowledge or suspicion is based, or which gives the reasonable grounds for that knowledge or suspicion, came to them in the course of the business and makes the SAR as soon as practicable after the information or other matter comes to them.

QUESTION: How do I submit a SAR (Disclosure) to the FIS?

ANSWER: A SAR must be submitted to a prescribed police officer at the FIS by using the online reporting facility known as 'THEMIS'.

QUESTION: How can I use the online reporting facility, THEMIS?

ANSWER: The online facility is accessed through the FIS website. To access this facility a person must register with the FIS. To enable this registration process, relevant contact details are required together with an authorisation should the required person be acting on behalf of a FSB or Non-FSB. A registration form can be found on our website. **www.guernseyfiu.gov.gg**

QUESTION: What should I include in a SAR?

ANSWER: The quality of a SAR is only as good as the content therefore you should include, 'who, what, where, when, why and how'. Include as much information as you can which has led to your suspicion; including all supporting documentation and any analysis undertaken.

QUESTION: What do I do if I am requested to provide additional information from the FIS?

ANSWER: FSBs who receive a Regulation 2 or a Regulation 2A from the FIS should respond as instructed by the FIS.

QUESTIONS & ANSWERS — SARS

PLEASE NOTE THAT THESE Q&As CONSTITUTE BRIEF GUIDANCE AND ARE PROVIDED FOR INFORMATION ONLY

QUESTION: If the SAR includes a reference to a specific transaction or activity that has led to the suspicion and ultimately a SAR, should the FSB request 'consent' to continue with the particular transaction or activity?

ANSWER: If the SAR does include reference to a specific transaction or activity that has led to the suspicion and ultimately a SAR; the FSB should indicate whether or not it intends to carry out the transaction or activity, and if so request 'consent' to continue with the particular transaction or activity.

The MLRO should exhaust all avenues at his disposal to either negate or confirm whether or not there is a suspicion before seeking 'consent' from the FIS. On receipt of such a request the FIS will consider whether or not it may give 'consent' under the relevant provisions.

In the event that 'consent' is not given, the FIS will discuss with the FSB the implications and will offer what assistance it can in deciding the most appropriate course of action to be taken thereafter. Any such discussion with the FIS does not constitute legal advice. If deemed appropriate, legal advice should be sought by the FSB from its Advocate or other legal advisor.

QUESTION: Can I terminate the business relationship?

ANSWER: Whether or not to terminate a business relationship is a commercial decision for the FSB. Where a FSB makes a decision to terminate a business relationship after it has made a SAR or requested consent and is concerned that in doing so it may prejudice an investigation or contravene the tipping off rules, it should engage with the FIS accordingly. The decision to terminate a relationship, however, remains with the FSB.

QUESTION: What is 'Tipping Off'?

ANSWER: The Disclosure Law, the Proceed of Crime Law and the Terrorism and Crime Law provide that it is a criminal offence if a person knows, or suspects, that an internal suspicion report to a MLRO or a SAR to the FIS has been or will be made or if any information or other matter concerning the internal suspicion report or SAR has been or will be communicated to a MLRO or the FIS and he discloses to any other person information or any other matter about, or relating to, that knowledge or suspicion unless it is for a purpose set out in those laws. Those purposes include, but are not limited to, the prevention, detection, investigation or prosecution of criminal offences, whether in the Bailiwick or elsewhere.

The HM Procureur has issued a paper entitled Guidance on Prosecution for Tipping Off which provides for disclosures made to members of the same organisation or linked organisation to discharge their AML/CFT responsibilities.

Reasonable enquiries of a customer, conducted in a discreet manner, regarding the background to a transaction of activity which has given rise to the suspicion is prudent practice, forms an integral part of CDD and ongoing monitoring, and should not give rise to tipping off.

QUESTIONS & ANSWERS — THEMIS

THEMIS — Online Reporting Facility for a Disclosure of Suspicion

This facility is for the creation and submission of a suspicious activity report/disclosure of suspicion of money laundering and/or terrorism financing to a prescribed police officer by virtue of Regulation 1 of The Disclosure (Bailiwick of Guernsey) Regulations, 2011 and The Terrorism and Crime (Bailiwick of Guernsey) Regulations, 2011.

PLEASE NOTE THAT THESE Q&As CONSTITUTE BRIEF GUIDANCE AND ARE PROVIDED FOR INFORMATION ONLY

QUESTION: As a MLRO for numerous entities, do I have to register all of my entities for THEMIS?

ANSWER: Yes. You are only required to advise the FIS of entities with a reporting responsibility. Any entities that will never have clients or deals with funds and will therefore never have a reason to report to the FIS do not need to register for THEMIS.

QUESTION: How do I submit additional information or an update on THEMIS?

ANSWER: Locate the SAR in your Disclosure Reports tab and select 'view', click on the 'further information' tab. Add the details of the additional information here.

QUESTION: I have extra documentation that I wish to add to a SAR I have already submitted. How do I do this?

ANSWER: To submit the 'additional documents';

i. Please click on the 'attachments' tab and attach the documents.

ii. Click on the 'further Information' tab. Include here details of the attached documents.

iii. Click 'submit'. This will notify the FIS that there is additional information.

QUESTION: When do I need to submit a new SAR?

ANSWER: A new SAR should be submitted for each new suspicion. If the suspicion remains the same and you have additional information to provide you should update the FIS with the additional information on the original SAR (see above).

QUESTION: Do I have to notify the FIS when I change roles within the same organisation?

ANSWER: No. MLRO, Deputy MLRO, Compliance Officers, Directors and Nominated Officer all have the same access on Themis when registered.

If you leave your current role for a different organisation or if you no longer require access to Themis, a registration form must be completed and signed by an authorised person as outlined on the form and returned to the FIS, indicating that you require your access to the system to be removed.

QUESTIONS & ANSWERS — THEMIS

PLEASE NOTE THAT THESE Q&As CONSTITUTE BRIEF GUIDANCE AND ARE PROVIDED FOR INFORMATION ONLY

QUESTION: Why do my entities in Themis have 'REP INST' or 'MLRO' written after them?

ANSWER: This is just an internal marker identifying the institution as a reporting institution and an individual as a reporting officer.

QUESTION: Can the FIS change my password?

ANSWER: No. Click on the 'forgotten password' link. Enter your username and registered email address carefully, and click 'submit'. If you see an error message, please contact the FIS at this point. You should receive a message informing you that a password reset message has been sent to the registered email address provided. Click on the 'reset password' link within the email. Enter your username details and enter a new password. Click 'save'.

After click 'save' you will be taken back to the main logon page.

Once your password has been reset successfully, you will receive a confirmation email to your registered email address.

Passwords must be at least 8 characters long, containing both letters and numbers and cannot be a repeat of your previous 5 passwords.

QUESTION: Why have I received multiple emails for the same notice?

ANSWER: If you are registered for more than one entity, you may receive multiple email notifications as an email is sent to all entities.

SAR TYPOLOGIES

Typology 1

An estate agent submitted a SAR to the FIS regarding an offer on a high value local property by person A, who advised that he wished to complete the purchase within a 4 week period. A month later, person A, who had not viewed the property had his offer accepted by the vendors.

The estate agent became suspicious of person A's behaviour. Due diligence was undertaken by legal firm A acting on behalf of person A and no transaction took place. Adverse open source identified a link with regards to theft, fraud and money laundering.

A second SAR was submitted from legal firm A reporting that person A wished to proceed with the purchase of the property. Due diligence identified adverse open source information and a social media page alleging that person A used a false UK address to prove his identity when registering with estate agents.

A third SAR was submitted by a legal firm B, who also had received an instruction to establish a business with the purpose of acquiring properties in the UK, advising that his business partner would be managing the business. Enhanced due diligence was requested in which person A failed.

Analysis was undertaken by the FIS who identified person A had a number of impending prosecutions in the UK for fraud. All intelligence was disseminated to the UK, and the FIS have received feedback that person A has been charged with approximately forty counts of making false representation to make gain for self or another and that the case was being sent for committal to the Crown Court.

Indicators: High value property, abnormal behaviour, open source material, social media, failure to provide due diligence.

Typology 2

The FIS received a SAR from a bank after person A paid in cash to their own account, and two further cash deposits into two separate third-party UK accounts. The cashier noted that the cash had an unusual odour, and therefore asked person A questions about the source of the funds. Person A was vague in answering.

Analysis on the UK account (person B) identified credits being received from a variety of locations, including person B's personal account at another bank, before being transferred to an account held by person C in another jurisdiction. Credits identified appeared to be linked to cash-intensive businesses. Analysis revealed that the credits greatly exceeded the level of credits expected through normal account activity.

Analysis identified that person B's account appears to be operating as a 'collection account' potentially for the purpose of money laundering. Enquiries are ongoing.

Indicators: Cash deposits, third-party accounts, unusual odour, vague behaviour, unusual account activity.

SAR TYPOLOGIES

Typology 3

An e-gaming entity submitted a SAR to the FIS and dual reported to the National Crime Agency (NCA) regarding a client who failed to satisfy enhanced due diligence on the source of funds that they had deposited into their e-gaming account. Analysis identified that the deposits made within a one month period greatly exceeded their annual salary. Documentation provided by the client revealed large amounts of payments were received from various persons. The e-gaming entity was unable to verify if these funds were derived from legitimate sources, and the account was suspended.

Analysis conducted by the FIS and the NCA identified that the subject had a conviction in June 2016 for theft from employer. The UK police confirmed that they would be seeking a restraint on the funds held in the account of the e-gaming entity. As a result of the confiscation hearing, a confiscation order was granted identifying a benefit figure of £35,000.

Indicators: Large deposits in a short period of time, large payments being received, failure to provide adequate verification of source of funds.

Typology 4

A trust and company service provider submitted a SAR after receiving an instruction to make two payments which purportedly originated from an authorised party to a trust relationship held at the trust and company service provider. During the process to validate the instructions authenticity, it was identified that the email address that the request originated from had been compromised.

Fraudulent triggering of both attempted and successful bank transactions have increased. In these cases hackers target the e-mail account of the victim and spy on it in order to send the bank payment instructions that look as authentic as possible. These can originate from a hacked or 'spoofed' email account or from similar email addresses of the victim.

To avoid a fraud being committed, if an unusual email request is received, verification steps should be taken via another channel to ensure that the email is a genuine email and not a fraudulent attempt.

Indicators: Characters substituted in email addresses, an urgency to complete a transaction, further email contact, unusual amounts, unusual jurisdictions, a new company or client.

Bailiwick of Guernsey Financial Intelligence Service Annual Report 2016

BAILIWICK OF GUERNSEY
LAW ENFORCEMENT