ISLE OF MAN
FINANCIAL SERVICES AUTHORITY
Lught-Reill Shirveishyn Argidoil Ellan Vannin

Preventing Financial Crime

Analysis of firms' data

(2017 and 2018)

BANKS

Published: March 2021

Contents

1. Introduction and Key Findings for Banks

1.1 This report is focused on those firms whose primary business is that of being a **Bank** (deposit taking). Reports for other sectors are also produced.

1.2 Generally, Banks in the Isle of Man provide a range of products and services to local and international customers. Such services include current and savings accounts, loans, foreign exchange and treasury services, and payments. Some also have permissions for investment business and general insurance. In the majority of cases, Banks are part of wider banking groups with the associated governance and control frameworks in place that come with such bigger entities.

1.3 This report provides an analysis of two years of data and covers areas such as the geographical profile of customers and beneficial owners, Banks' assessment of customer risk, reporting and monitoring of financial crime and sanctions, and the use of introducers and third parties.

1.4 **Table 1** below provides information on the population of **Banks** who were required to submit the annual AML/CFT data return for December 2018 and December 2017.

Table 1: Population of banks for the purpose of this Report

	December 2018	**December 2017**
Number of Banks	12	13

1.5 The analysis confirms that the client base is diverse, with a wide geographical spread of customers by residency, beneficial ownership and location of activity (for example where funds flow to and from). There is therefore a significant cross border aspect to the Island's banking sector. The data also confirms that a substantial portion of business is conducted on a non face to face basis, with some also through introducers. Banks also reported that they do undertake business with foreign PEPs.

1.6 The above profile, coupled with the nature of products and services offered by Banks results in a higher inherent risk of Banks being exposed to a range of money laundering, terrorist financing, and sanctions threats. The importance of Banks having strong and effective monitoring and control frameworks is therefore paramount.

2. Background to the AML/CFT data return

2.1 The Isle of Man Financial Services Authority's ("the Authority") regulatory objectives[1] include *"the reduction of financial crime"*. In its **2018-2021 Strategic Plan** the Authority sets out its *long term goals* and *strategic objectives* which include:-

Long term goal	Strategic objective
Continue to develop our identity and culture and to operate as a forward looking integrated regulator	*Enhance the framework to protect consumers and deter financial crime*
Fully implement a risk-based supervisory approach for every entity within our remit, including vulnerability to financial crime	*Encourage innovation and continuous improvement in all that we do*
Be an International Financial Centre which is recognised as effectively deterring financial crime	

2.2 During 2016-2017 the Authority consulted on, and subsequently introduced, a pilot annual AML/CFT data return, designed to obtain information from regulated and registered entities to help the Authority monitor AML/CFT threats and trends in, and across, sectors. The table below shows the scope of returns to date and the planned returns for submission in 2020 and thereafter:

Responders	Annual reporting period	Basis for the information	Submission deadline
All regulated entities[2] Sample of registered entities[3]	31 December 2016	Best endeavours[4]	29 November 2017
All regulated and registered entities (firms)	31 December 2017	Part actual data, part best endeavours	31 December 2018
All firms	31 December 2018	Part actual data, part best endeavours	31 December 2019
All firms	31 December 2019	Part actual data, part best endeavours	30 September 2020, contingency to 31 December 2020
All firms	31 December 2020 and thereafter	Actual data (unless by exception)	30 June 2021 and 30 June thereafter

2.3 Based on the original pilot exercise (December 2016 data), high level results were presented to industry groups during 2018. The Authority has now also analysed the

[1] as set out in the Financial Services Act 2008 ("FSA08")
[2] Regulated under the FSA08, the Insurance Act 2008 and the Retirement Benefits Schemes Act 2000
[3] Registered under the Designated Businesses (Registration and Oversight) Act 2015.
[4] Refer Annex 1: Data Quality.

2017 and 2018 data and developed, for the first time, a collective industry view across sectors[5], excluding gambling, that are subject to the Island's AML/CFT framework. The Authority will use this information to help with its risk assessment of sectors, and individual firms.

3. Objectives

3.1 The gathering and analysis of data from all firms about AML/CFT helps the Authority to achieve the regulatory objective of "*the reduction of financial crime*".

3.2 The data informs the Authority's understanding of the ***inherent risks*** that firms, and sectors, may pose, and supports the Authority's AML/CFT supervisory work utilising a risk based approach. Some information provided also relates to a firm's ***control environment***. The information that must be reported is dependent on the type of activity a firm undertakes, for example a bank must report more information when compared to a financial advisory firm. Key areas of focus include:-

- The jurisdictional risk profile of the customer base and ultimate beneficial owners;
- The extent of non-face to face and introduced business undertaken by firms;
- Identification and reporting of suspicious activity for both money laundering and terrorist financing;
- Monitoring and screening processes adopted, including for sanctions;
- How firms categorise customer risk;
- The level of politically exposed persons in the system, and how these are identified;
- The compliance and internal audit mechanisms;
- Outsourcing of AML/CFT processes;
- The payment methods accepted by firms in relation to incoming and outgoing transfers; and
- The types of client or product / services provided.

3.3 The data underpins the Island's understanding of the wider financial crime environment and forms a key part of the National Risk Assessment process, alongside the specific quarterly financial flow data that the Authority receives from the Island's banking sector.

[5] The data does not include information from the small number of firms who are regulated only for bureau de change, agency payment services, or cheque cashing. These firms currently submit different AML/CFT statistical data which is analysed separately.

4. Customer risk profile – Banks

A. Geographical profile - residency

4.1 Firms are required to report their customer relationships according to the residency of the customer, based on the ISO country code standard. This information enables the Authority to consider jurisdictional risk, and the extent to which customers are linked to higher-risk jurisdictions, when assessing sectors and firms.

4.2 The total number of customer[6] relationships reported by Banks as at 31 December 2018 was **635,937** (***2017: 560,968***), of which **25.8%** are resident in the Isle of Man (***2017: 23.7%***) and **21.7%** in the UK (***2017: 23.2%***).

At the end of 2018, Banks reported that **90.9%** of customers were natural persons (***2017: 94.3%***). Of the natural persons, **21.9%** are resident in the Isle of Man (***2017: 22.5%***) and **22.5%** in the UK (***2017: 23.5%***). Some of these customers will be customers of more than one firm that reports data.

Of the non-natural persons, the most common residency (of the legal arrangement) was the Isle of Man at **64.9%** (***2017: 43.6%***). The UK and the Channel Islands made up a further **27.0%** (***2017: 41.8%***).

The data reported by Banks on the residency of non-natural customers (legal arrangements) is not unexpected with the majority being from countries which have mature company and trust formation sectors. Further, Banks reported that **25.4%** of their non-natural customer book were customers introduced by Isle of Man regulated trust and company service providers (***2017: 20.1%***).

Note: one bank was unable to report only Isle of Man situs customer data and instead reported data for the bank as a whole, including its business in the Channel Islands. This bank is a material reporter.

Tables 2a and 2b below provide a more detailed breakdown.

[6] It should be noted that the quality of reporting varies across banks between "customers" and "accounts" for this purpose, and there are differences in treatment for 2017 and 2018.

Table 2a: Total percentage of relationships based on residency of the customer

	Customer relationships: natural persons (% of total customers)		Customer relationship: Non-natural persons[7] (% of total customers)		Total customer relationships (% of total)	
	2018	**2017**	**2018**	**2017**	**2018**	**2017**
Isle of Man	19.9%	21.2%	5.9%	2.5%	25.8%	23.7%
Channel Islands	12.8%	12.7%	1.2%	1.2%	14.0%	13.9%
UK	20.5%	22.2%	1.2%	1.0%	21.7%	23.2%
EU (excludes EEA and Switzerland)	9.8%	8.9%	0.2%	0.3%	10.0%	9.2%
Other Europe	1.1%	1.2%	0.1%	0.1%	1.2%	1.3%
Africa	9.9%	11.0%	0.1%	0.2%	10.0%	11.2%
Americas	6.4%	6.7%	0.3%	0.2%	6.7%	6.9%
Asia (including Middle East)	7.0%	7.3%	0.1%	0.1%	7.1%	7.4%
Oceania	3.5%	3.1%	0.0%	0.1%	3.5%	3.2%
TOTAL	**90.9%**	**94.3%**	**9.1%**	**5.7%**	**100%**	**100%**

Table 2b: Top 10 countries by residency of the customer

Country of residence	Natural Persons (% of total natural persons)		Country of residence	Non-natural persons (% of total non-natural)	
	2018	**2017**		**2018**	**2017**
UK	22.5%	23.5%	Isle of Man	64.9%	43.6%
Isle of Man	21.9%	22.5%	UK	13.5%	18.2%
Jersey	8.9%	8.5%	Guernsey	6.1%	12.8%
South Africa	7.4%	8.3%	Jersey	7.4%	10.8%
Guernsey	5.2%	4.9%	BVI	1.2%	1.7%
USA	3.9%	4.0%	Cyprus	0.9%	1.6%
Australia	2.5%	2.4%	South Africa	0.5%	0.9%
United Arab Emirates	2.1%	2.2%	Ireland	0.5%	0.9%
Spain	2.1%	1.9%	Cayman Islands	0.7%	0.8%
France	2.1%	1.8%	Malta	0.5%	0.7%
TOTAL	**78.6%**	**80.0%**		**96.2%**	**92.0%**

Note that there were no changes in the top 10 list from 2017 to 2018.

[7] For a corporate or trust customer the residency will likely be reported as the country of incorporation / establishment of that company or trust (or of the trustee).

4.3 In summary, the jurisdictional profile of the customer base for **Banks** is wide in its scope and therefore there is a resultant increased inherent risk of being exposed to a range of money laundering / terrorist finance threats.

Also see **section 5E** for information on banks' payment flows.

B. Geographical profile – residency of ultimate beneficial owners

4.4 Banks also provide services to non-natural customers ("entities") and must understand who the beneficial owners of such entities are.

Of the non-natural customer book, **41.7%** of beneficial owners are resident in the UK ***(2017: 29.8%)***, followed by the Isle of Man at **28.5%** (***2017: 40.2%)***.

Note: some banks were not able to report complete residency data on beneficial owners of non-natural customers. Further, one bank (a material reporter) was not able to report any data for 2017, and for 2018 its data was based on the residency of all key account parties (i.e. including directors) and was therefore excluded for analysis purposes.

Tables 3a and 3b below provide a more detailed breakdown

Table 3a: Residency of the beneficial owners of non-natural customers

	Residency at December 2018		Residency at December 2017	
	Beneficial owners	Entities	Beneficial owners	Entities
Isle of Man	28.5%	64.9%	40.2%	43.6%
Channel Islands	0.5%	13.5%	0.5%	23.6%
UK	41.7%	13.5%	29.8%	18.2%
EU (excludes EEA and Switzerland)	8.0%	2.3%	8.5%	4.4%
Other Europe	3.3%	0.6%	4.2%	1.4%
Africa	7.1%	1.4%	5.7%	2.4%
Americas	4.6%	2.8%	4.6%	4.4%
Asia (including Middle East)	5.6%	0.9%	6.1%	1.7%
Oceania	0.7%	0.1%	0.4%	0.3%
TOTAL	**100%**	**100%**	**100%**	**100%**

Table 3b: Top 10 countries by residency of the beneficial owner (of entities)

	Country of residence of the beneficial owner (% of total number of beneficial owners)	
	2018	2017
Isle of Man	28.5%	40.2%
UK	41.7%	29.8%
South Africa	4.2%	3.2%
Italy	1.5%	2.0%
Switzerland	1.4%	1.5%
United Arab Emirates	1.3%	1.4%
USA	1.3%	1.3%
Gibraltar (not in top 10 for 2018)	-	1.1%
Brazil (not in top 10 for 2018)	-	1.0%
Cyprus	1.3%	1.0%
Ireland (new in top 10 for 2018)	1.2%	-
Kenya (new in top 10 for 2018)	1.2%	-
TOTAL	**83.6%**	**82.5%**

The jurisdictional profile of the beneficial owners of non-natural customers for **Banks** is relatively wide in its scope, albeit with a particular concentration of UBOs being resident in the Isle of Man and UK (**circa 70%**).

4.5 Similar to the residency profile for customers who are natural persons, the range of residency of UBOs is relatively wide in scope and therefore there is a resultant increased inherent risk of Banks being exposed to a range of money laundering / terrorist finance threats, including through more complex structures. Also see **section 5E** for information on banks' payment flows.

C. Politically exposed persons and other high risk customers

4.6 **Tables 4a and 4b** show customer relationships, as assessed by Banks, deemed to pose a higher risk of money laundering, and the level of politically exposed persons ("PEPs") among the customer base. PEPs[8] include people with prominent public jobs who may be in a position to abuse their role for private gain.

4.7 At the end of 2018 Banks reported **1,702 customers who are, or are associated with, a PEP**[9] (***2017: 1,649***), including **1,318 related to foreign PEPs** (***2017: 1,224***). Firms are required to identify PEPs at the start of a business relationship and, through effective monitoring, if any persons subsequently become PEPs. Firms are required by law to undertake enhanced checks and monitoring of all customers who are, or are

[8] PEP is defined in the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019.
[9] The actual number of individual (natural) PEPs may be lower than the number of customers reported.

associated with, foreign PEPs and any domestic PEPs who the Firm assesses as posing a higher risk.

Table 4a: PEP relationships

	Number of PEP relationships (and as a % share of all relationships)	
	As at December 2018	As at December 2017
Customer who are, or are associated with, politically exposed persons (PEPs)	1,702 (0.27%)	1,649 (0.29%)
Of which are foreign PEPs	*1,318*	*1,224*
Of which are domestic PEPs	*384*	*425*

4.8 At the end of 2018 (and 2017), **all** Banks confirmed that they screen for PEPs at the commencement of a business relationship, and screen their customer records on a periodic basis to determine if a customer has become a PEP. For the latter the frequency of screening was generally daily for all customer risk types; noting one bank reported it screens weekly, and one reported it only screens on an annual basis.

4.9 At the end of 2018 Banks reported they had **14,659 higher risk customers** (***2017: 15,275***); this includes customers who are categorised as being higher risk for reasons other than being a PEP. Where firms identify that customers pose a higher risk, either at the outset of a business relationship, or through an event that occurs during the business relationship, they are legally required to conduct enhanced customer due diligence.

Note: one bank was unable to report only Isle of Man situs customer data (for the purpose of risk categories) and instead reported data for the bank as a whole, including its business in the Channel Islands. This bank is a material reporter.

Table 4b: High-risk customer relationships

	Number of high risk customer relationships (total and new) (and as a % share of total / new customer relationships[10])	
	December 2018	December 2017
Total high risk customers (*includes any PEPs assessed as higher risk*)	14,659 (2.31%)	15,275 (2.72%)

[10] Some banks reported new customer relationship data based on number of new accounts, rather than unique customer numbers.

New high risk customers on-boarded in the reporting period (*includes any PEPs assessed as higher risk*)	1,973 (3.45%)	4,300 (7.7%)

4.10 Overall, PEPs and other high risk customers represent a **relatively small proportion** of the total customer base of Banks (**less than 3%**). Note that the same individual customers may appear more than once in these figures because individuals and businesses may have multiple financial relationships.

4.11 The number of new high risk customers on-boarded, as a proportion of all new customers on-boarded, decreased in 2018 compared to 2017. The figure in 2017 included over 3,000 reported by one bank, which had decreased to circa 800 in 2018.

4.12 Banks also reported that they review the customer risk assessment and CDD information for all high risk (including higher risk PEPs) relationships at least annually.

5. Tackling Financial Crime – Banks

A. Resourcing the fight against financial crime

5.1 To effectively monitor and address the risk that persons abuse the financial system for money laundering and terrorist financing requires a significant amount of firms' time and resources. As at 31 December 2018 Banks reported that they collectively employ **2,060 staff in the Isle of Man** (***2017: 2,040***), of which **96 (5%)** were reported as being in compliance and prevention of financial crime roles (***2017: 95 / 5%***).

It should be noted that compliance roles are not solely focused on financial crime. Banks also reported **8 FTE compliance / financial crime vacancies** at the end of 2018 (***2017: 10***).

5.2 Relevant staff require ongoing training to ensure they have the effective knowledge to help detect and prevent their firm from being misused by criminals. In the year ended 31 December 2018, Banks reported that **2,065 general refresher training places were filled** (***2017: 1,591***). This effectively represented **100%** of total staff employed (including directors) (***2017: 78%***).

In addition, Banks reported that **407 staff** (**20%**) received additional specialist training (**2017: 224 / 11%**).

B. Outsourcing of processes to group entities or third parties

5.3 Information is obtained on the outsourcing of certain activities or functions to group entities or third parties. Where outsourcing occurs firms should have robust monitoring and control processes in place, as responsibility remains with the firm. Information is requested in respect of the following:-

- Customer on-boarding (including for risk assessments, collection of due diligence, screening, and business acceptance);
- Ongoing monitoring;
- MLRO and Compliance activity (for AML/CFT); and
- Staff screening and take-on.

5.4 It was evident from the reporting by Banks that they outsource a range of activity relating to the above, including within their wider groups and, to a more limited extent, third parties. The most extensive use of outsourcing was for the screening of staff at take-on, and the least use was, as expected, for MLRO and Compliance activity. **Table 5** below provides more information (for 2018 only).

Table 5: Outsourcing of AML/CFT activity

Description	**Undertaken by the Bank**	**Outsourced to Group**	**Outsourced to Third Parties**
Client on-boarding[11]			
Customer risk assessments	Yes - all	Yes - 2	Yes - 1
Collection of customer due diligence	Yes - all	Yes - 3	Yes - 3
Customer screening	Yes - all	Yes - 1	Yes - 1
Customer acceptance[12]	Yes - all	Yes - 1	Yes - 1
Ongoing monitoring	Yes - all	Yes - 2	Yes - 2
MLRO & Compliance activity[13]			
MLRO / DMLRO activity	Yes – except 1	Yes - 1	No
Compliance activity	Yes – except 2	Yes - 3	No
Staff screening and take-on[14]	Yes - 7	Yes - 8	Yes - 6

[11] Outsourcing may be for only customer segments or part of a process.
[12] Outsourcing of business acceptance was for very specific purposes, and subject to the consent of the Authority.
[13] Any outsourcing was intra-group within the Isle of Man.
[14] All 5 Banks which did not undertake this "in-house" reported that they outsourced to their groups. A range of Banks also outsourced part of the process to third parties.

C. Monitoring for, and reporting of, financial crime

5.5 The law requires employees of firms to report knowledge or suspicion of money laundering within their firm, to their MLRO. In the year ended 31 December 2018, **1,163** cases of concern, suspicion or knowledge of money laundering were either identified by staff, generated through automated processes, or identified from other intelligence sources, and reported to the firms' MLROs (***2017: 1,357***). In addition, a further **1** report was raised which was terrorism related (***2017: 3***).

5.6 MLROs must consider these reports, and decide whether a formal submission to the **Isle of Man Financial Intelligence Unit**[15] ("FIU") is justified, and must be registered with the FIU's "Themis" system to be able to make reports. At the end of 2017 and 2018, all Banks reported they were registered on "Themis".

5.7 In 2018, after investigation by MLROs, **519** cases of knowledge or suspicion of money laundering were reported to the FIU (***2017: 813***). **No** reports were made that were terrorism related (***2017: 2***). Further, Banks reported **66** cases to the FIU regarding general intelligence (***2017: 26***).

5.8 In 2018 Banks also handled **349** requests from law enforcement and other competent authorities (***2017: 270***). Of these, **276** explicitly related to money laundering (***2017: 193***) and **1** for terrorism (***2017: 1***).

5.9 Engagement between the FIU, other law enforcement agencies and financial firms is a crucial component that supports investigations and prosecutions, not only in the Isle of Man but as part of international cooperation. It is evident that Banks form a significant part of this infrastructure.

Table 6: Liaising with the authorities

Description	**Year ended 31 Dec 2018**	**Year ended 31 Dec 2017**
Number of internal Money Laundering disclosures to the MLRO	1,163	1,357
Number of external Money Laundering disclosures to the FIU	519	813
Number of internal Terrorist Financing disclosures to the MLRO	1	3
Number of external Terrorist Financing disclosures to the FIU	0	2
Section 24 disclosures to the FIU	66	26
Enquiries received from law enforcement authorities	**244**	**219**

[15] See https://www.fiu.im/

Of which were Money Laundering related	234	188
Of which were Terrorism related	1	1
Enquiries received from other competent authorities	**105**	**51**
Of which were Money Laundering related	42	5
Of which were Terrorism related	0	0

D. Refusing and blocking services because of financial crime risk

5.10 Concerns relating to financial crime may lead to firms turning away a prospective customer. In the year ended 31 December 2018 Banks reported they **declined 65** potential new relationships because of financial crime, terrorism or sanctions related concerns (***2017: 169***). In some cases, Banks would not always have knowledge or suspicion of financial crime but customers may have posed an unacceptable risk.

Of the declined cases, **80%** were natural persons resident outside the Isle of Man (***2017: 83%***).

The total number of **declined cases** equated to **less than 0.5%** of all new customer relationships established for both 2017 and 2018.

Table 7b provides a further breakdown.

5.11 Firms are required to monitor ongoing business relationships and may cease to provide services because of their own financial crime risk appetite, or may terminate relationships under certain circumstances, including liaising with the FIU if a matter is subject to "consent"[16]. During the year ended 31 December 2018 Banks **terminated 253** existing relationships because of financial crime, terrorism or sanctions related concerns (***2017: 207***).

Of the terminated cases, **61%** were natural persons resident outside the Isle of Man (***2017: 74%***).

The total number of **terminated cases** equated to **less than 0.5%** of all customer relationships that were closed or terminated for both 2017 and 2018.

Table 7b provides a further breakdown.

[16] Section 154 of the Proceeds of Crime Act provides a reporting mechanism called "an authorised disclosure", which is a means by which a defence against money laundering can be obtained by a firm. Making an authorised disclosure can be used as the vehicle to seek consent to commit a prohibited act (i.e. possessing, acquiring, moving known or suspected criminal property).

5.12 In addition to terminating relationships, firms may be requested by law enforcement agencies to block or freeze accounts, or may themselves put additional controls around accounts if information is required from a customer. As at the end of 2018 there were **130 accounts blocked or frozen** for money laundering or terrorism (***2017: 96***).

Table 7a: disrupting provision of services - summary

Description	Year ended 31 Dec 2018		Year ended 31 Dec 2017	
	Number	Asset Value £'000	Number	Asset Value £'000
Number of potential new customer relationships declined for ML/FT or sanctions purposes	65		169	
Number of customer relationships terminated for ML/FT or sanction purposes	253		207	
Blocked or frozen accounts for AML/CFT purposes – subject to consent including restraint orders etc.	130	38,098	96	14,511
Blocked or frozen accounts for any other purpose (e.g. gone away)	1,140[17]	14,822	111	911

Note: not all banks were able to accurately report the number and value of "blocked or frozen accounts for any other purpose.

Table 7b: disrupting provision of services – declined and terminated business for ML/FT or sanctions purposes

Description	Declined		Terminated	
	2018	2017	2018	2017
Natural persons IOM	6	4	62	26
Natural persons non-IOM	52	141	154	153
Charities - IOM	0	0	0	0
Charities – non IOM	0	0	0	0
Corporate / trust – managed by IOM TCSPs	0	8	15	4
Corporate / trust - other	7	16	22	24
Other customers	0	0	0	0
TOTAL	**65**	**169**	**253**	**207**

[17] A key reason for this increase is due to a change in reporting by one bank which changed systems and undertook a full mailing exercise of customers. This has resulted in additional accounts being temporarily blocked.

E. The Isle of Man banking system as gatekeeper

5.13 When it comes to the material flow of funds into and out of the Island, the banking sector plays an important gatekeeper role. Data on the monetary value and volume of inflows and outflows for banks including origin and destination of funds is provided to the Authority quarterly, and shared with the FIU. The first complete annual data of sufficient quality was for 2018. The Authority uses the payment flow data to help inform its risk assessment of Banks and consider thematic or Bank specific supervisory review work. **Table 8** below provides a breakdown by geographic region.

Table 8: Payment flows[18] (based on cumulative data to Dec 2018 data, 12 months)

	12mth Inflows Value £billion (%)	**12mth Outflows Value £billion (%)**
TOTAL ALL COUNTRIES	**77.0**	**67.6**
Of which UK	42.8 (55%)	35.5 (53%)
Of which inter IOM	2.3 (3%)	2.2 (3%)
Of which Channel Islands	5.3 (7%)	2.9 (4%)
Of which EU	10.1 (13%)	9.2 (14%)
Of which other Europe	2.6 (3%)	2.9 (4%)
Of which Americas	9.4 (12%)	8.5 (12%)
Of which Africa	2.1 (3%)	2.7 (4%)
Of which Asia (incl. Middle East)	2.1 (3%)	3.1 (5%)
Of which Oceania	0.3 (less than 0.5%)	0.6 (1%)
Highest risk countries (29)	**12mth Inflows**	**12mth Outflows**
Total value £billion	0.25	0.30
As a % of total flow	*0.32%*	*0.44%*

5.14 98% of all inflows and 96% of all outflows are to or from jurisdictions of lower or at least equivalent level of risk to the UK, which is the largest trading partner of the Isle of Man. In 2018 **2%** of all inflows and **4%** of outflows were connected to **higher risk jurisdictions**[19]. However, only **0.32%** of all inflows and **0.44%** of all outflows were from / to the **29 highest risk countries**. The payment data is not inconsistent with the geographic spread of the customer base of Banks.

[18] Payment Flow data is not fully complete, for example not all banks are reporting sterling flows in faster payments / bacs.
[19] For the purposes of this report, higher risk jurisdictions (including those considered the *highest risk*) are those identified by the Authority via a composite rating derived from the higher of the Aon Risk Index scores and the Basle AML/CFT index.

5.15 The largest inflows from the highest risk countries were from Kenya. Nigeria was the second highest. In line with incoming financial flows, Kenya was the highest risk jurisdiction which received most of the overall outflow, taking in 0.24% of all funds leaving the IoM (and the 31st highest receiver of IoM outflow overall). The second highest was Turkey. Mozambique, Uganda, Tanzania, and Lebanon, were also identified. As the Isle of Man has some banks which are part of African headquartered banking groups, these flows are not unexpected.

5.16 For the receipt and withdrawal / movement of funds into / out of bank accounts, banks reported that the predominant methods used were bank transfer, cheques, and debit card. Credit cards, payment providers (e.g. Paypal) and bankers' drafts were also used.

5.17 **6 Banks** also reported that the acceptance and payment of cash is usual, and **2 Banks** reported it was occasional or by exception. Strong controls, monitoring and appropriate limits around the use of cash is therefore important to help prevent lower level domestic laundering.

6. Managing and reporting of sanctions – Banks

6.1 It is important that firms have robust controls in place to ensure they comply with local and international sanctions. In order to help achieve this firms must have appropriate monitoring and screening tools to identify whether any of their customers (existing or prospective) are sanctioned individuals or organisations, and also to make sure funds paid / received are not made to / from sanctioned individuals or organisations.

6.2 At the end of 2018, **all** Banks confirmed that they screen for sanctions at the commencement of a business relationship, and screen their customer records on a periodic basis to determine if a customer has become subject to sanctions (which includes terrorism lists). For the latter, the frequency of screening was predominantly daily (through automated monitoring), with the exception of one bank which reported it screened weekly.

6.3 At the end of 2018, for outward and inward payments, Banks reported the following information in relation to screening for sanctions:-

<u>SWIFT (international) payments</u>

- For outward payments **all** relevant Banks screen in real time or prior to the payment being released – this screening was for the sender of the payment, the beneficiary, and other relevant parties.

- For inward payments **all** relevant Banks screen in real time (with one exception, which was "after event") – this screening was for the remitter, the beneficiary, and other relevant parties. Banks also reported that they monitor incoming payments for complete payer / payee information (as required under wire transfer regulations) either in real time or after event.

BACS and Faster Payments (sterling domestic payments only[20])

Banks reported that they generally **do not** screen UK sterling payments (in and out) for sanction purposes. There were however some exceptions to this reported by 4 Banks, noting some screening of senders, remitters and beneficiaries (in and out).

6.4 There is always potential that firms hold the funds of sanctioned individuals or organisations, mainly because such individuals / organisations will not have been subject to sanctions when they were originally accepted as a customer. In such cases, firms may be required to block or freeze assets for financial sanctions purposes. As at the end of 2018 there were **22 accounts blocked or frozen** for financial sanctions purposes (***2017: 13***) with an aggregate value of **£4.2 million** (***2017: £3.7million***).

6.5 The law requires firms to identify and report any suspected breach of sanctions[21] to the **Financial Intelligence Unit**. In practice, these reports will be made by a firm's MLRO or Deputy MLRO using Themis (with processes in place internally for employees to report to the MLRO / Deputy MLRO). In the year ended 31 December 2018, **1 disclosure** was made for suspected breaches of sanctions (***2017: 7***).

Table 9: managing and reporting sanctions

Description	31 Dec 2018		31 Dec 2017	
	Number	Asset Value £'000	Number	Asset Value £'000
Number of disclosures made for suspected breach of sanctions	1		7	
Accounts blocked or frozen in the year for financial sanctions purposes	20	1,572	12	529
Blocked or frozen accounts for financial sanctions purposes released in the year	0	0	0	0
Number and value of blocked or frozen accounts for financial sanctions purposes as at the year end	22	4,200	13	3,669

[20] Domestic means Isle of Man, UK, Gibraltar and Channel Islands for this purpose.
[21] With reference to the "Sanctions List", which means the list of persons who are currently subject to international sanctions which apply in the Isle of Man: this list is maintained by the Customs and Excise Division of the Treasury of the Isle of Man.

7. Delivery of services: face to face, use of introducers and third parties – Banks

7.1 How a firm delivers its products and services to customers can range from direct relationships with face to face interaction before a business relationship is established, or an occasional transaction conducted, to situations where relationships are established remotely directly by the customer, or through introducers / third parties (and sometimes through more than one layer of introducer / third party).

7.2 In 2018, Banks reported **57,242** new relationships (***2017: 55,536***). The actual number of unique new customers is lower than the above numbers as some banks reported this data on an "account" basis.

7.3 On a unique customer basis Banks reported **29,356** new customers in 2018 (***2017: 42,623***). Of these new customers, **56%** was reported as direct business (***2017: 65%***), whereas introduced business accounted for **33%** (***2017: 34%***).

7.4 In 2018, on a "best endeavours basis", Banks reported that **55%** of new customers were either met by the Bank or a related party to the Bank (***2017: 42%***), and **45%** relationships were established on a non face to face basis (including through introducers) (***2017: 56%***).

7.5 For introduced business, the main source of introductions were from Isle of Man Based TCSPs, group offices, and in one case overseas financial advisory firms. For customers introduced to Banks, the top 5 residency of the introducers (in terms of the number of clients introduced) for both 2018 and 2017 were:-

- Isle of Man
- UK
- South Africa
- United Arab Emirates
- France

Even where introducers are utilised, Banks reported that, in many cases, they obtain evidence of verification of identity of the customer from the introducer, rather than utilising the concessions available in law (relying on the introducer to hold that evidence, where an introducer is eligible to do so).

Annex 1 – Data Quality

The following matters should be noted in relation to the data provided in this report:-

- Parts of some firms' data is provided on a "best endeavours basis" and therefore cannot be considered as 100% accurate.
- The figures for customer numbers, including PEPs, is based on a simple sum of individual firms' data. A customer of one firm may also have relationships with another and be counted twice in this data.
- One Bank was unable to report only Isle of Man situs customer data and instead reported data for the bank as a whole, including its business in the Channel Islands. This bank is a material reporter.
- The quality of reporting varies across Banks between "customers" and "accounts" for various data sets, and there are also differences in treatment for 2017 and 2018.
- Banks' capability to accurately report the split of new business between those established on a face to face versus non-face to face varies, as does the ability to report introduced business information.