

KEY FINANCIAL SECRECY INDICATORS

Key Financial Secrecy Indicator 1: Banking Secrecy

What is measured?

This indicator assesses whether a jurisdiction provides banking secrecy. We go beyond the statutory dimension to assess the absence or inaccessibility of banking information and the criminalisation of breaches as elements of banking secrecy. For a jurisdiction to obtain a zero secrecy score on this indicator, it must ensure that banking data exists, that it has effective access to this data and that it does not sanction breaching of banking secrecy with prison term sentences. We consider that effective access exists if the authorities can obtain account information without the need for separate authorisation, for example, from a court, and if there are no undue notification requirements or appeal rights against obtaining or sharing this information.


Accordingly, we have split this indicator into six subcomponents; the overall secrecy score for this indicator is calculated by simple addition of these sub-components. The secrecy scoring matrix is shown in Table 1, with full details of the assessment logic given in Table 5 below.


In order to determine whether a jurisdiction's law includes the possibility of imprisonment or custodial sentencing for breaching banking secrecy, we rely on responses to the TJN-survey and analyse each country's relevant laws to the extent this is feasible. Unless we are certain that a jurisdiction may not punish breaches of banking secrecy (for example, by a potential whistle-blower) with prison terms, we add a 20% secrecy score.

The availability of relevant banking information is measured by a jurisdiction's compliance with FATF-recommendations 5 and 10.¹ Recommendation 5 states that "financial institutions should not keep anonymous accounts or accounts in obviously fictitious names". The recommendation specifies that the financial institution must be able to identify not just the legal owner but also the beneficial owner(s), both in the case of natural and legal persons.² If a jurisdiction fails to comply with this recommendation, this adds a 20% secrecy score.³

FATF-recommendation 10 requires financial institutions to "maintain, for at least five years, all necessary records on transactions, both domestic and international".⁴ A further 20% secrecy score is added if a jurisdiction is non-compliant with this recommendation. We have relied on the mutual evaluation reports by the FATF, FATF-like regional bodies, or the IMF for the assessment of these two criteria.⁵

Table 1: Secrecy Scoring Matrix KFSI 1

Dimensions	Component	Secrecy Score Assessment (Sum = 100%, fully secretive)	Source(s) FSI database  (Including references per jurisdiction for IDs 89, 157, 158, 352, 353 and 360)
Consequences of breaching banking secrecy	(1) Breaching banking secrecy may lead to imprisonment / custodial sentencing, or unknown	20%	Individual research for each country / TJN-Survey
Availability of relevant information	(2) Anonymous accounts – FATF Rec. 5, or unknown	20%	FATF, FATF-like regional bodies, or IMF
	(3) Keep banking records for less than five years – FATF Rec. 10, or unknown	20%	
	(4) No reporting of large transactions, or unknown	20%	Bureau for International Narcotics and Law Enforcement Affairs (INCSR)
Effective access	(5) Inadequate powers to obtain and provide banking information, or unknown	10%	Global Forum peer reviews elements B.1 and B.2 (incl. factors and text)
	(6) Undue notification and appeal rights against information exchange, or unknown	10%	


All underlying data can be accessed freely in the [FSI database](#) . To see the sources we are using for particular jurisdictions please consult the assessment logic in Table 5 at the end of this document and search for the corresponding info IDs (**IDs 89, 157, 158, 352, 353, 360**) in the database report of the respective jurisdiction.

In addition, and in order to diversify our sources, we have also used data contained in the International Narcotics Control Strategy Report (INCSR, Volume 2 on Money Laundering and Financial Crimes).⁶ This report indicates for a wide selection of countries whether banks are required to report large transactions. Failure to do so is assessed as an additional 20% secrecy score.⁷

However, since it is not sufficient for banking data to merely exist, we also measure whether this data can be obtained and used for information exchange purposes, and if no undue notification⁸ requirements or appeal rights⁹ prevent effective sharing of banking data. We rely on the Global Forum’s element B.1¹⁰ for addressing the first issue at hand (powers to obtain and provide data), and we use Global Forum’s element B.2¹¹ for the second issue (notification requirements/appeal rights). Each will be attributed a 10% secrecy score if any qualifications apply to the elements and underlying factors¹². An overview of the rating for B.1 and B.2 is given in Table 2:

Table 2: Assessment of Global Forum Data for KFSI 1

“Determination”¹³ Results as in table of determinations of Global Forum B.1 / B.2	“Factors”¹⁴ Results as in table of determinations of Global Forum B.1 / B.2	Secrecy Score
“The element is in place.”	No factor mentioned.	0%
“The element is in place.”	Any factor mentioned.	10%
“The element is in place, but certain aspects of the legal implementation of the element need improvement.”	Irrelevant.	10%
“The element is not in place.”	Irrelevant.	10%

All underlying data can be accessed freely in the [FSI database](#)  (IDs 89, 157, 158, 352, 353 and 360).

Why is this important?

For decades, factual and formal banking secrecy laws have obstructed information gathering requests from both national and international competent authorities such as tax administrations or financial regulators. Until 2005, most of the concluded double [tax agreements](#)¹⁵ did not specifically include provisions to override formal banking secrecy laws when responding to information requests by foreign treaty partners.

This legal barrier to accessing banking data for information exchange purposes has been partially overcome with the [advent of automatic information exchange](#)¹⁶. Automatic exchange of information (AEOI) following the OECD's Common Reporting Standard (CRS) got underway in 2017 (see [KFSI 18](#)¹⁷). However, we consider access to information and undue notifications related to the "Upon Request" standard to be relevant still for the following reasons. First, AEOI will not take place among all countries. If AEOI takes place between countries A and B, country C (very likely a developing country) will still depend on specific information requests for accessing banking information from countries A or B. Second, AEOI will complement but not replace exchanges upon request. For example, after countries A and B exchange banking information automatically, country A may need to obtain more detailed information (e.g. when the account was opened, what was the highest balance account or a specific transaction). All these extra details will not be included in AEOI, but will have to be asked via specific requests. In other words, even when AEOI is fully implemented and involves all countries, exchanges upon request will remain necessary.

In addition, some jurisdictions have tightened their penalties for breaches of extant banking secrecy. For example, in September 2014, Switzerland passed a law that extended the prison sentence for whistle-blowers who disclose bank data from three years to a maximum of five years. The prison terms had previously been increased with effect from 1 January 2009.¹⁸

Some countries even defend their banking secrecy laws by means of criminal law and concomitant prosecution. Such laws intimidate and silence bank insiders who are ideally placed to identify dubious or clearly illegal activities by customers and/or collusion by bank staff and/or management. Effective protection for whistle-blowers, which allows them to report to domestic or foreign authorities, and/or to the media about a bank customer's illegal activities, is necessary to ensure that banking secrecy does not enable individuals, companies and banks to jointly and systematically break the law.

The extent to which banking secrecy has acted as a catalyst for crime became evident through recent leaks and large scale public prosecutions of banks that have engaged in and supported money laundering and tax evasion by clients. In this context, the threat of prison sentences for breaches of banking secrecy has served to effectively deter, silence, retaliate against, and prosecute whistle-blowers, up to the point of issuing arrest warrants against officials from tax administrations, and deploying spies.¹⁹ The threat of criminal prosecution for breaches of banking secrecy was, and remains, a potent means of covering up illicit and / or illegal activity.

Another fashionable way²⁰ of achieving *de facto* banking secrecy consists of not properly verifying the identity of both account holders and beneficial owners, or allowing nominees such as custodians, trustees, or foundation council members to be acceptable as the only natural persons on bank records. Furthermore, the absence of or neglect in enforcing record keeping obligations for large transactions, for instance through wire transfers, is another way in which banks are complicit in aiding their clients to escape investigation.

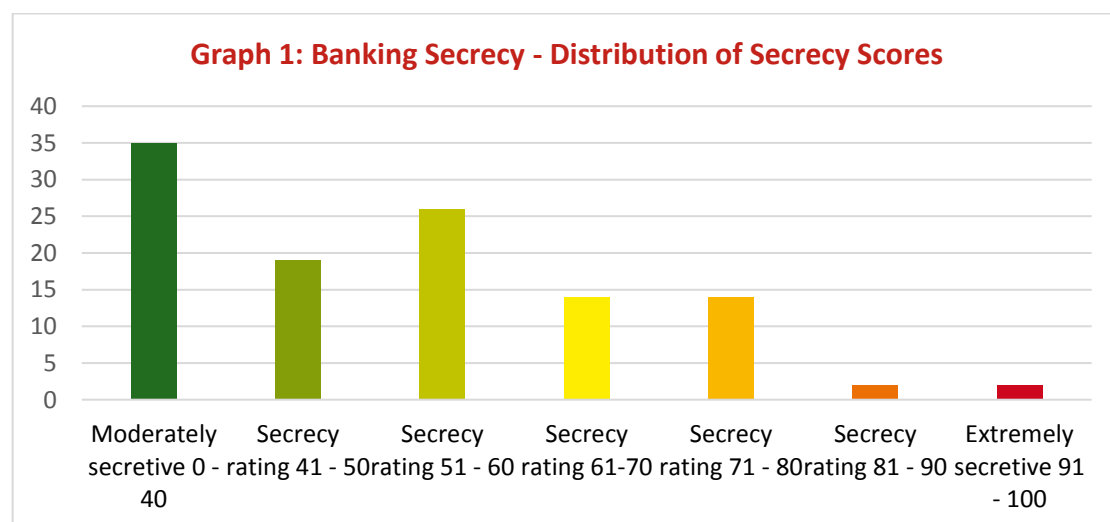
Since most trusts, shell companies, partnerships and foundations need to maintain a bank account for their activities, the beneficial ownership information banks are required to keep is often the most effective means of identifying the natural persons behind these legal structures. Together with the recorded transfers, ownership records of bank accounts can provide key evidence of criminal or illicit activity of individuals, such as embezzlement, illegal arms trading or tax fraud. Therefore, it is of utmost importance that authorities with appropriate confidentiality provisions in place can access relevant banking data routinely without being constrained by additional legal barriers, such as notification requirements, or factual barriers, such as missing or outdated records.

All underlying data can be accessed freely in the [FSI database](#) 📖 (IDs 89, 157, 158, 352, 353, 360).

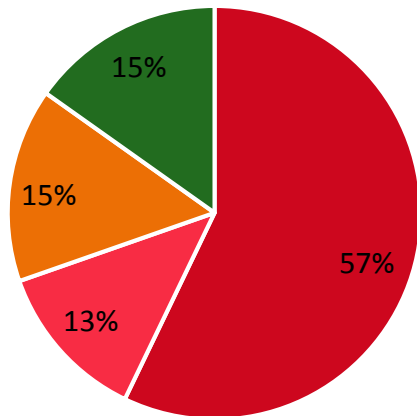
Results Overview

Table 3: Banking Secrecy Results - Overview

	Number
Jurisdictions rated moderately secretive 0 - 40	35
Jurisdictions with secrecy rating 41 - 50	19
Jurisdictions with secrecy rating 51 - 60	26
Jurisdictions with secrecy rating 61-70	14
Jurisdictions with secrecy rating 71 - 80	14
Jurisdictions with secrecy rating 81 - 90	2
Jurisdictions rated extremely secretive 91 - 100	2



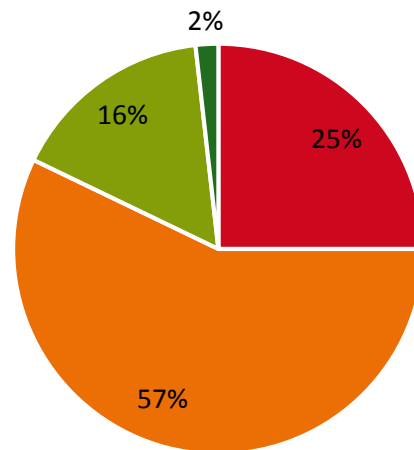
Graph 2: Statutory Sanctions for Breaches of Banking Secrecy



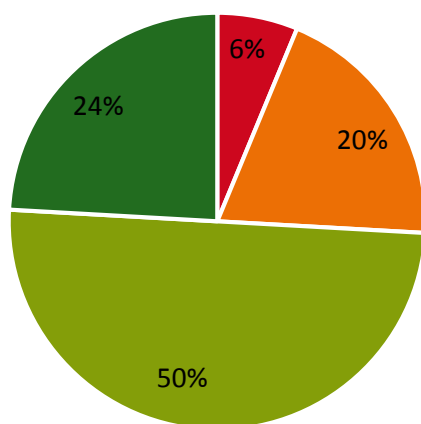
- Prison terms for disclosing client's banking data to any third party (and possibly fines)
- Unkown: inconclusive statutory provisions and/or no answer to TJN Survey
- Fines for disclosing client's banking data to any third party, but no prison terms
- No statutory sanctions for disclosing client's banking data to any third party

Graph 3: Are banks subject to stringent customer due diligence regulations? (FATF old R5, new R10)

- Not at all: AD, AE, AW, BM, BN, BW, BZ, DM, GD, GH, HR, JP, KE, KN, LC, LR, MK, MV, NZ, PL, PY, SC, SM, TC, TH, TR, TZ, VC
- Partially: all other jurisdictions
- Largely: AT, BE, CA, CR, EE, ES, FR, GG, GT, IE, IM, IT, ME, MT, PT, SE, SI, TT
- Fully: Malaysia and Singapore



Graph 4: Are banks required to maintain data records of its customers and transactions sufficient for law enforcement? (FATF old R10, new R11)



- Not at all: AG, BB, BW, LC, MV, SM, TZ
- Partially: BN, BZ, DO, GH, GI, GM, HK, IL, KE, LR, LV, MK, PA, PL, PY, RO, SC, TC, TH, TW, VE, ZA
- Largely: all other jurisdictions
- Fully: AT, BE, CH, CR, DM, ES, FI, GB, GG, GT, IS, IT, JE, LB, LI, LT, MT, MX, PT, SA, SE, SG, SI, TR, TT, UY, WS

Table 4: Banking Secrecy Scores

Country Name	Score	ISO	Country Name	Score	ISO
Andorra	0,87	AD	Lebanon	0,73	LB
Anguilla	0,7	AI	Liberia	0,53	LR
Antigua & Barbuda	0,93	AG	Liechtenstein	0,73	LI
Aruba	0,57	AW	Lithuania	0,13	LT
Australia	0,2	AU	Luxembourg	0,6	LU
Austria	0,57	AT	Macao	0,6	MO
Bahamas	0,7	BS	Macedonia	0,33	MK
Bahrain	0,8	BH	Malaysia (Labuan)	0,27	MY
Barbados	0,53	BB	Maldives	0,8	MV
Belgium	0,07	BE	Malta	0,47	MT
Belize	0,73	BZ	Marshall Islands	0,3	MH
Bermuda	0,67	BM	Mauritius	0,6	MU
Bolivia	0,6	BO	Mexico	0,43	MX
Botswana	0,6	BW	Monaco	0,5	MC
Brazil	0,5	BR	Montenegro	0,54	ME
British Virgin Islands	0,4	VG	Montserrat	0,8	MS
Brunei	0,63	BN	Nauru	0,4	NR
Bulgaria	0,3	BG	Netherlands	0,5	NL
Canada	0,14	CA	New Zealand	0,27	NZ
Cayman Islands	0,4	KY	Norway	0,2	NO
Chile	0,6	CL	Panama	0,56	PA
China	0,4	CN	Paraguay	0,73	PY
Cook Islands	0,5	CK	Philippines	0,5	PH
Costa Rica	0,37	CR	Poland	0,53	PL
Croatia	0,37	HR	Portugal (Madeira)	0,37	PT
Curacao	0,6	CW	Puerto Rico	0,6	PR
Cyprus	0,5	CY	Romania	0,46	RO
Czech Republic	0,4	CZ	Russia	0,3	RU
Denmark	0,6	DK	Samoa	0,63	WS
Dominica	0,7	DM	San Marino	0,6	SM
Dominican Republic	0,56	DO	Saudi Arabia	0,43	SA
Estonia	0,24	EE	Seychelles	0,73	SC
Finland	0,53	FI	Singapore	0,4	SG
France	0,54	FR	Slovakia	0,5	SK
Gambia	0,66	GM	Slovenia	0,07	SI
Germany	0,5	DE	South Africa	0,26	ZA
Ghana	0,53	GH	Spain	0,07	ES
Gibraltar	0,76	GI	St Kitts and Nevis	0,77	KN
Greece	0,6	GR	St Lucia	0,7	LC
Grenada	0,77	GD	St Vincent & Grenadines	0,67	VC
Guatemala	0,37	GT	Sweden	0,27	SE
Guernsey	0,57	GG	Switzerland	0,73	CH
Hong Kong	0,86	HK	Taiwan	0,66	TW
Hungary	0,7	HU	Tanzania	1	TZ
Iceland	0,33	IS	Thailand	0,73	TH
India	0,4	IN	Trinidad & Tobago	0,47	TT
Indonesia	0,5	ID	Turkey	0,7	TR
Ireland	0,24	IE	Turks & Caicos Islands	0,73	TC
Isle of Man	0,44	IM	Ukraine	0,4	UA
Israel	0,56	IL	United Arab Emirates (Dubai)	0,47	AE
Italy	0,27	IT	United Kingdom	0,43	GB
Japan	0,27	JP	Uruguay	0,53	UY
Jersey	0,43	JE	US Virgin Islands	0,4	VI
Kenya	0,63	KE	USA	0,2	US
Korea	0,5	KR	Vanuatu	0,4	VU
Latvia	0,66	LV	Venezuela	0,56	VE

Moderately Secretive 0 – 0,4	Secrecy Score 0,41 – 0,50	Secrecy Score 0,51 – 0,60	Secrecy Score 0,61 – 0,70	Secrecy Score 0,71 – 0,80	Secrecy Score 0,81 – 0,90	Extremely Secretive 0,91 – 1
---------------------------------	------------------------------	------------------------------	------------------------------	------------------------------	------------------------------	---------------------------------

Table 5: Assessment Logic

Info_ID	Text_Info_ID	Answers (Codes applicable for all questions: -2: Unknown; -3: Not Applicable)	Valuation % Secrecy
360	Criminal sanctions, custodial sentencing or any other statutory sanctions for breaches of banking secrecy?	0: Yes, there are prison terms for disclosing client's banking data to any third party (and possibly fines); 1: Yes, there are fines for disclosing client's banking data to any third party, but no prison terms; 2: No, there are no statutory sanctions for disclosing client's banking data to any third party.	20% unless answer is >0
352	To what extent are banks subject to stringent customer due diligence regulations ("old" FATF-recommendation 5/"new" 10)?	0: Fully; 1: Largely; 2: Partially; 3: Not at all.	20% pro rata
353	To what extent are banks required to maintain data records of their customers and transactions sufficient for law enforcement ("old" FATF-recommendation 10/"new" recommendation 11)?	0: Fully; 1: Largely; 2: Partially; 3: Not at all.	20% pro rata
89	Are banks and/or other covered entities required to report large transactions in currency or other monetary instruments to designated authorities?	Y/N	20% if N, or -2
157	Sufficient powers to obtain and provide banking information on request?	1: Yes without qualifications; 2: Yes, but some barriers; 3: Yes, but major barriers; 4: No, access is not possible, or only exceptionally.	10% except if answer is 1
158	No undue notification and appeal rights against bank information exchange on request?	1: Yes without qualifications; 2: Yes, but some problems; 3: Yes, but major problems; 4: No, access and exchange hindered.	10% except if answer is 1

¹ These recommendations refer to the 49 FATF recommendations of 2003. While the FATF consolidated its recommendations to a total of 40 in 2012, the old recommendations are used here because the assessment of compliance with the new recommendations only began in 2013. The corresponding recommendations in the new 2012 set of recommendations are numbers 10 (replacing old Rec. 5) and 11 (replacing old Rec. 10). FSI 2017 takes into account the results of the new assessments. The old recommendations can be viewed at: www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf; 01.06.2015; the new recommendations are available at: www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf; 20.10.2016.

² www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf; 20.10.2016. Also see footnote above.

³ In order to measure compliance, the FATF uses the following scale: 0 = non-compliant; 1 = partially compliant; 2 = largely-compliant; 3 = fully compliant. We attribute a 20% secrecy score for non-compliant, 13% for partially compliant, 7% for largely compliant and zero secrecy for fully compliant answers.

⁴ www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf; 01.06.2015. Also see footnote above.

⁵ For the purposes of this subcomponent of the KFSI, we ignored the follow-up reports to mutual evaluations, and instead only included the results of full mutual evaluation reports. This is because only a comprehensive re-assessment of all recommendations gives a complete picture of the anti-money laundering system and offers a fair basis for comparison across jurisdictions. Otherwise, potential deteriorations in formerly compliant elements of recommendations might go unnoticed, while the improvements in formerly non-compliant criteria will be focused upon.

⁶ While we would have liked to include the data from the 2017 INCSR report, unfortunately this report discontinued that data field (together with many others) in its reporting. Therefore, we have used the 2016 edition of the INCSR, see note below.

⁷ The information is presented in the table on pages 7-17 under the column “Report Large Transactions”, in: <https://www.state.gov/documents/organization/258726.pdf>; 13.10.2017.

⁸ While the Global Forum peer reviews assess whether a notification (to the beneficial owner) could delay or prevent the exchange of information, we also consider whether any notification to the owner takes place at all, even if it is after the exchange of information, because the owner could start taking actions (transfer assets, leave the country, etc.) to obstruct the legal and economic consequences of the requesting jurisdiction’s investigation or proceedings. By being made aware, owners could also take precautionary measures with respect to assets, bank accounts, etc., located in other jurisdictions.

⁹ In those cases when the owner is not notified (either because it is not a legal requirement or because there are exceptions to this notification), we still evaluate whether the information holder has any right to appeal or to seek judicial review. In this case, we consider whether there are legally binding timeframes for the appeal procedures and appropriate confidentiality safeguards which would ensure that the exchange of information would not be delayed or prevented.

¹⁰ The full element B.1 reads as follows: “Competent authorities should have the power to obtain and provide information that is the subject of a request under an exchange of information arrangement from any person within their territorial jurisdiction who is in possession or control of such information (irrespective of any legal obligation on such person to maintain the secrecy of the information).” (See page 27 in: Global Forum on Transparency and Exchange of Information for Tax Purposes 2010: Implementing the Tax Transparency Standards. A Handbook For Assessors and Jurisdictions, Paris).

¹¹ The full element B.2 reads as follows: “The rights and safeguards (e.g. notification, appeal rights) that apply to persons in the requested jurisdiction should be compatible with effective exchange of information.” (See page 28, in Global Forum 2010, op. cit.).

¹² Because under Global Forum’s methodology there are no clear criteria to determine when identified problems as described in “factors” are going to affect the assessment of an “element”, we refrain from assessing a secrecy score only if no problems (factors) have been identified, irrespective of the element’s assessment. However, we do consider both: (i) whether the factors mentioned are related to bank information; and (ii) whether information described in the report (even if not mentioned as a factor) is also relevant to assess a jurisdiction’s power to obtain and exchange bank information. Also see footnotes below for more background.

¹³ The Global Forum peer review process analyses and determines whether the ten elements considered necessary by the OECD for “upon request” information exchange are in place. A three-tier assessment is available (element “in place”, “in place, but”, “not in place”), and this assessment is called “determination”. See footnote above and below for more details.

¹⁴ Each of the “determinations” (as explained in footnotes above) of the ten elements may have underlying factors which justify the element’s determination and the recommendations given. They are shown in a column next to the determination in the “table of determinations” in the corresponding peer review reports.

¹⁵ https://www.taxjustice.net/cms/upload/pdf/Tax_Information_Exchange_Arrangements.pdf

¹⁶ Meinzer, Markus 2017: Automatic Exchange of Information as the New Global Standard: The End of (Offshore Tax Evasion) History?, in: SSRN Electronic Journal, in: <http://www.ssrn.com/abstract=2924650>; 21.7.2017.

¹⁷ <http://www.financialsecrecyindex.com/PDF/18-Automatic-Info-Exchange.pdf>; 8.8.2017.

¹⁸ See page 17, in: Meinzer, Markus 2015: Steueroase Deutschland. Warum bei uns viele Reiche keine Steuern zahlen, München.

¹⁹ <http://www.taxjustice.net/2017/06/02/whistleblower-ruedi-elmer-vs-swiss-justice-system/>; <http://www.spiegel.de/wirtschaft/soziales/schweizer-geheimdienst-sammelte-informationen-ueber-deutsche-steuerfahnder-a-1145703.html>; 21.7.2017.

²⁰ <http://www.sueddeutsche.de/politik/mittelamerika-leticia-und-diebriefkasten-oma-1.2954968>; www.taxjustice.net/cms/upload/pdf/TJN_1110_UK-Swiss_master.pdf; <https://www.ifc.org/wps/wcm/connect/62d48198-f722-48f0-80fc-172e68649bdd/Focus-14.pdf?MOD=AJPERES>; 8.8.2017.