

## 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 1.1, with full details of the assessment logic given in Table 1.4 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 points of secrecy score.

The availability of relevant banking information is measured by a jurisdiction's compliance with FATF-recommendations 5 and 10.<sup>1</sup> 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.<sup>2</sup> If a jurisdiction fails to comply with this recommendation, this adds a 20 points of secrecy score.<sup>3</sup>

FATF-recommendation 10 requires financial institutions to "maintain, for at least five years, all necessary records on transactions, both domestic and

# KFSI 1: BANKING SECRECY

international”.<sup>4</sup> A further 20 points of 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.<sup>5</sup>

**Table 1.1: Secrecy Scoring Matrix KFSI 1**

<b>Regulation</b>	<b>Secrecy Score Assessment</b> [Secrecy Score: 100 points = full secrecy; 0 points = full transparency]
<b>Component 1: Consequences of breaching banking secrecy (20 points)</b>	
(1) Breaching banking secrecy may lead to imprisonment / custodial sentencing, or unknown	20
<b>Component 2: Availability of relevant information (60 points)</b>	
(2)(a) Anonymous accounts – FATF Rec. 5, or unknown	20
(2)(b) Keep banking records for less than five years – FATF Rec. 10, or unknown	20
(2)(c) No reporting of large transactions, or unknown	20
<b>Component 3: Effective access (20 points)</b>	
(3)(a) Inadequate powers to obtain and provide banking information, or unknown	10
(3)(b) Undue notification and appeal rights against information exchange, or unknown	10

**All underlying data can be accessed freely in the [Financial Secrecy Index database](#).** To see the sources we are using for particular jurisdictions please consult the assessment logic in Table 1.5 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).<sup>6</sup> This report indicates for a wide selection of countries whether banks are required to report large transactions<sup>7</sup>. Failure to do so is assessed as an additional 20 points of secrecy score.<sup>8</sup>

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 notification<sup>9</sup> requirements or appeal rights<sup>10</sup> prevent effective sharing of banking data. We rely on the Global Forum’s element B.1<sup>11</sup> for addressing the first issue at hand (powers to obtain and provide data), and we use Global Forum’s element B.2<sup>12</sup> for the second issue (notification requirements/appeal rights). Each will be attributed a 10 points secrecy score if any qualifications apply to the elements and underlying factors.<sup>13</sup> Where available, we also consider countries’ replies to TJN-survey 2019.<sup>14</sup>

We consider that sufficient powers to obtain and provide banking information on request is applied if the jurisdiction’s authorities are able to access banking information which is at least 5 years old. For example, for FSI 2020, if a country is not able to access banking information from 2014 but is able to do so regarding banking information from 2016, than we would consider the ability to obtain and provide banking information to be sufficient.

An overview of the rating for B.1 and B.2 is given in Table 1.2:

**Table 1.2: Assessment of Global Forum Data for KFSI 1**

<b>“Determination”<sup>15</sup></b>	<b>“Factors”<sup>16</sup></b>	<b>Secrecy Score</b>
Results as in table of determinations of Global Forum B.1 / B.2	Results as in table of determinations of Global Forum B.1 / B.2	
“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 [Financial Secrecy Index 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](#)<sup>17</sup> 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](#)<sup>18</sup>. Automatic exchange of information (AEOI) following the OECD's Common Reporting Standard (CRS) got underway in 2017 (see [KFSI 18](#)<sup>19</sup>). 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.<sup>20</sup>

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.<sup>21</sup> 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 way<sup>22</sup> 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.

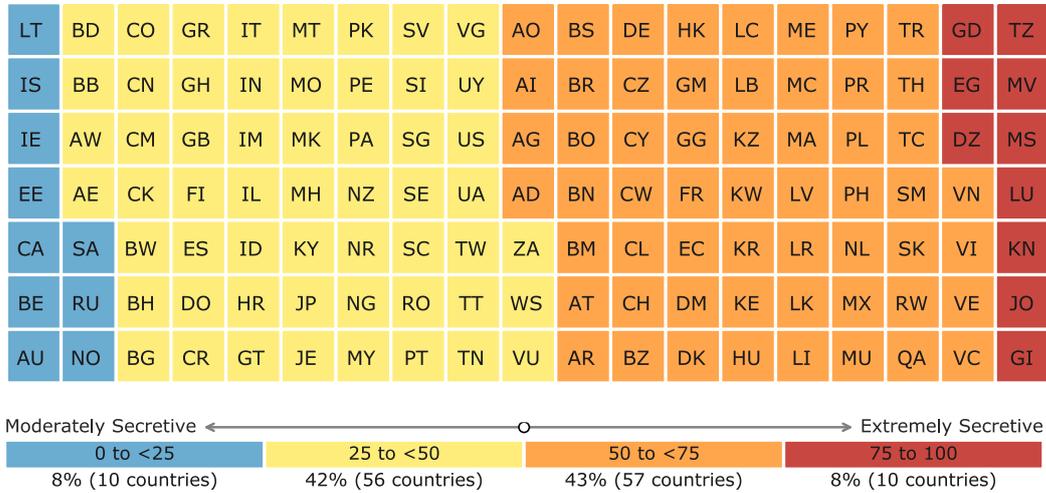
Since most trusts, shell companies, partnerships and foundations need to maintain a bank account for their activities, the beneficial ownership information banks are required to keep is often the most effective means of identifying the natural persons behind these legal structures. Together with the 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  [Financial Secrecy Index database](#) (IDs 89, 157, 158, 352, 353, 360).**

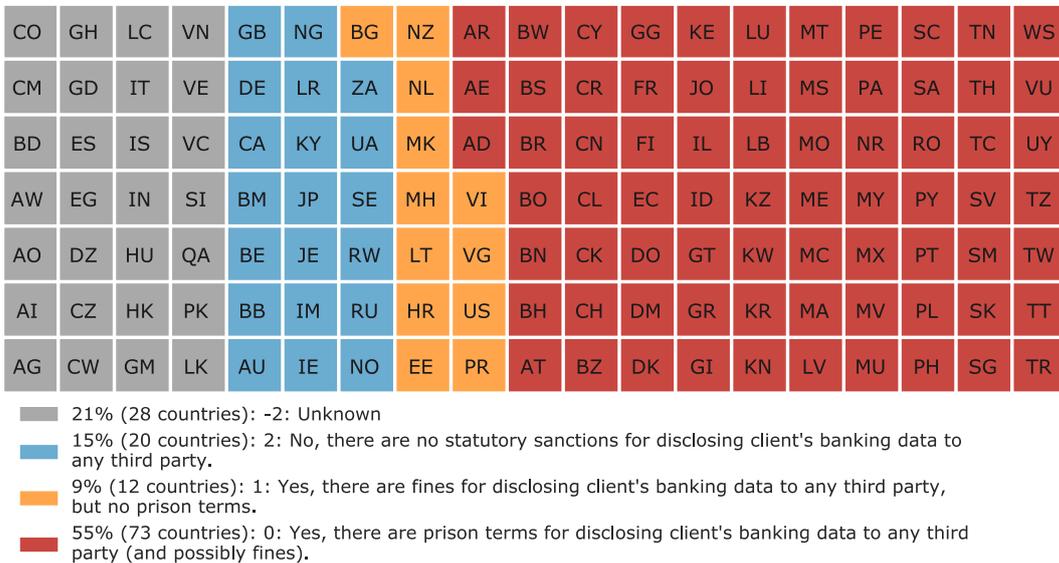
# KFSI 1: BANKING SECRECY

## Results Overview

**Figure 1.1: Banking secrecy-distribution of secrecy scores**

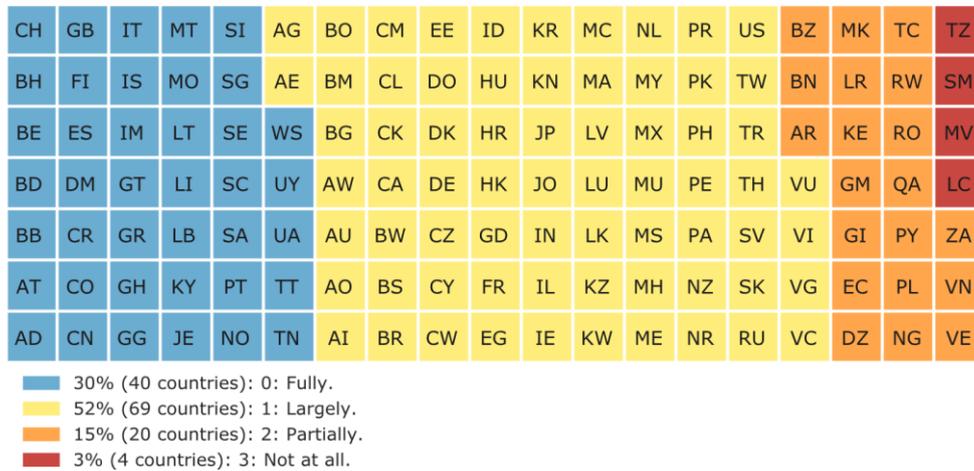


**Figure 1.2: COMPONENT 1: Are there criminal sanctions, custodial sentencing or any other statutory sanctions for breaches of banking secrecy? (ID 360)**



# KFSI 1: BANKING SECRECY

**Figure 1.3: COMPONENT 2(a): To what extent are banks required to maintain data records of its customers and transactions sufficient for law enforcement (old FATF-recommendation 10 / new FATF recommendation 11)? (ID 353)**



**Figure 1.4: COMPONENT 2(b): To what extent are banks subject to stringent customer due diligence regulations (Old FATF-recommendation 5 / new FATF-recommendation 10)? (ID 352)**

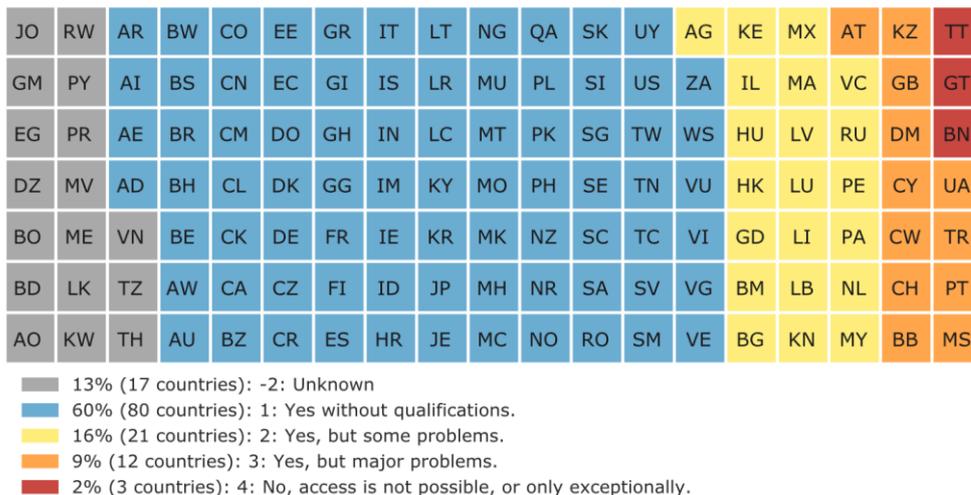


# KFSI 1: BANKING SECRECY

**Figure 1.5: COMPONENT 2(c): Are banks and/or other covered entities required to report large transactions in currency or other monetary instruments to designated authorities? (ID 89)**



**Figure 1.6: COMPONENT 3(a): Does the domestic administration have sufficient powers to obtain and provide banking information on request? (ID 157)**



# KFSI 1: BANKING SECRECY

**Figure 1.7: COMPONENT 3(b): Are there no undue notification and appeal rights against bank information exchange on request? (ID 158)**

GM	PR	VN	BH	CO	FI	ID	KN	MK	NL	PL	SE	VG	BB	ES	LC	SG	CL	UY
EG	MV	VE	BG	CN	DO	HR	KE	MA	NG	PK	SC	TW	AI	EE	KR	MS	CH	UA
EC	ME	TZ	AW	CM	DM	GR	JP	LT	MY	PE	SA	TR	AG	DE	JE	MH	BE	TT
DZ	LK	TN	AU	CA	DK	GH	IT	LR	MX	PA	RU	TC	AD	CK	IM	MC	VI	PH
BO	KW	TH	AT	BZ	CZ	GD	IS	LB	MU	NZ	RO	SV	ZA	BS	IE	LV	VC	HU
BD	JO	RW	AR	BW	CY	GB	IN	KZ	MT	NR	QA	SM	WS	BR	HK	LU	US	GI
AO	GT	PY	AE	BN	CR	FR	IL	KY	MO	NO	PT	SI	VU	BM	GG	LI	SK	CW

- 16% (21 countries): -2: Unknown
- 55% (73 countries): 1: Yes without qualifications.
- 22% (29 countries): 2: Yes, but some problems.
- 8% (10 countries): 3: Yes, but major problems.

# KFSI 1: BANKING SECRECY

**Table 1.3: Banking Secrecy Scores**

Secrecy score	ISO2: Country Name	Secrecy score	ISO2: Country Name
47	AW: Aruba	77	KN: St. Kitts and Nevis
60	AO: Angola	50	KR: South Korea
70	AI: Anguilla	67	KW: Kuwait
57	AD: Andorra	63	LB: Lebanon
47	AE: United Arab Emirates	53	LR: Liberia
53	AR: Argentina	70	LC: St. Lucia
74	AG: Antigua and Barbuda	73	LI: Liechtenstein
20	AU: Australia	54	LK: Sri Lanka
50	AT: Austria	7	LT: Lithuania
10	BE: Belgium	80	LU: Luxembourg
47	BD: Bangladesh	60	LV: Latvia
30	BG: Bulgaria	40	MO: Macao
47	BH: Bahrain	70	MA: Morocco
57	BS: Bahamas	50	MC: Monaco
73	BZ: Belize	80	MV: Maldives
67	BM: Bermuda	50	MX: Mexico
60	BO: Bolivia	30	MH: Marshall Islands
50	BR: Brazil	33	MK: Macedonia
27	BB: Barbados	47	MT: Malta
63	BN: Brunei	54	ME: Montenegro
40	BW: Botswana	80	MS: Montserrat
14	CA: Canada	54	MU: Mauritius
73	CH: Switzerland	37	MY: Malaysia
50	CL: Chile	33	NG: Nigeria
27	CN: China	50	NL: Netherlands
47	CM: Cameroon	7	NO: Norway
44	CK: Cook Islands	40	NR: Nauru
33	CO: Colombia	27	NZ: New Zealand
27	CR: Costa Rica	40	PK: Pakistan
60	CW: Netherlands Antilles	44	PA: Panama
27	KY: Cayman Islands	44	PE: Peru
50	CY: Cyprus	50	PH: Philippines
54	CZ: Czechia	53	PL: Poland
50	DE: Germany	60	PR: Puerto Rico
70	DM: Dominica	37	PT: Portugal
54	DK: Denmark	73	PY: Paraguay
34	DO: Dominican Republic	73	QA: Qatar
93	DZ: Algeria	46	RO: Romania
56	EC: Ecuador	24	RU: Russia
80	EG: Egypt	53	RW: Rwanda
37	ES: Spain	20	SA: Saudi Arabia
24	EE: Estonia	30	SG: Singapore
47	FI: Finland	40	SV: El Salvador
54	FR: France	60	SM: San Marino
37	GB: United Kingdom	70	SK: Slovakia
57	GG: Guernsey	27	SI: Slovenia
27	GH: Ghana	27	SE: Sweden
76	GI: Gibraltar	47	SC: Seychelles
66	GM: Gambia	73	TC: Turks and Caicos Islands
40	GR: Greece	54	TH: Thailand
77	GD: Grenada	40	TT: Trinidad and Tobago
47	GT: Guatemala	37	TN: Tunisia
74	HK: Hong Kong	64	TR: Turkey
27	HR: Croatia	34	TW: Taiwan
74	HU: Hungary	100	TZ: Tanzania
34	ID: Indonesia	27	UA: Ukraine
37	IM: Isle of Man	43	UY: Uruguay
40	IN: India	30	US: United States
24	IE: Ireland	67	VC: St. Vincent & Grenadines
20	IS: Iceland	56	VE: Venezuela
44	IL: Israel	40	VG: British Virgin Islands
27	IT: Italy	50	VI: US Virgin Islands
43	JE: Jersey	73	VN: Vietnam
80	JO: Jordan	34	VU: Vanuatu
27	JP: Japan	47	WS: Samoa
57	KZ: Kazakhstan	26	ZA: South Africa
63	KE: Kenya		



# KFSI 1: BANKING SECRECY

**Table 1.4: Assessment Logic**

<b>Info_ID</b>	<b>Text_Info_ID</b>	<b>Answers (Codes applicable for all questions: -2: Unknown; -3: Not Applicable)</b>	<b>Valuation Secrecy Score</b>
<b>360</b>	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 points unless answer is >0
<b>352</b>	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 points pro rata
<b>353</b>	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 points pro rata
<b>89</b>	Are banks and/or other covered entities required to report large transactions in currency or other monetary instruments to designated authorities?	Y/N	20 points if N, or -2
<b>157</b>	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 points except if answer is 1
<b>158</b>	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 points except if answer is 1

## Reference List

- Brinkmann, Bastian, Obermaier, Frederik, and Bastian Obermayer, 'Wie Einfache Bürger Billige Dienste Für Offshore-Kunden Leisten', *Süddeutsche.De* (18 April 2016) <<http://www.sueddeutsche.de/politik/mittelamerika-leticia-und-die-briefkasten-oma-1.2954968>> [accessed 29 January 2020]
- Der Spiegel, 'Schweizer Geheimdienst Sammelte Informationen Über Deutsche Steuerfahnder', 2 May 2017 <<https://www.spiegel.de/wirtschaft/soziales/schweizer-geheimdienst-sammelte-informationen-ueber-deutsche-steuerfahnder-a-1145703.html>> [accessed 29 January 2020]
- European Parliamentary Research Service - EPRS, 'Fighting Tax Crimes: Ex-Post Evaluation of the Cooperation between Financial Intelligence Units' (2017) <[http://www.europarl.europa.eu/RegData/etudes/STUD/2017/598603/EPRS\\_STU\(2017\)598603\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2017/598603/EPRS_STU(2017)598603_EN.pdf)> [accessed 29 January 2020]
- Financial Action Task Force, *Financial Action Task Force on Money Laundering. The Forty Recommendations.*, 2003 <<http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf>> [accessed 29 January 2020]
- , *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations (2012 - Updated 2019)* (Paris, June 2019) <<https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>> [accessed 29 January 2020]
- Fowler, Naomi, 'Whistleblower Rudolf Elmer: Legal Opinion on Latest Ruling', 2019 <<https://www.taxjustice.net/2019/06/04/whistleblower-rudolf-elmer-legal-opinion-on-latest-ruling/>, <https://www.taxjustice.net/2019/06/04/whistleblower-rudolf-elmer-legal-opinion-on-latest-ruling/>> [accessed 29 January 2020]
- Meinzer, Markus, 'Automatic Exchange of Information as the New Global Standard: The End of (Offshore Tax Evasion) History?', *SSRN Electronic Journal*, 2017 <<http://www.ssrn.com/abstract=2924650>> [accessed 29 January 2020]
- , *Steueroase Deutschland: Warum Bei Uns Viele Reiche Keine Steuern Zahlen* (Munich, 2015)
- Tax Justice Network, 'Financial Secrecy Index 2020 Questionnaire' <[https://www.financialsecrecyindex.com/PDF/FSI2020\\_Questionnaire-MOF-NAO.xlsx](https://www.financialsecrecyindex.com/PDF/FSI2020_Questionnaire-MOF-NAO.xlsx)> [accessed 29 January 2020]

- , 'Key Financial Secrecy Indicator 18: Automatic Information Exchange', 2020 <<http://www.financialsecrecyindex.com/PDF/18-Automatic-Info-Exchange.pdf>> [accessed 29 January 2020]
- , 'Tax Information Exchange Arrangements', 2009 <[http://www.taxjustice.net/cms/upload/pdf/Tax\\_Information\\_Exchange\\_Arrangements.pdf](http://www.taxjustice.net/cms/upload/pdf/Tax_Information_Exchange_Arrangements.pdf)> [accessed 24 January 2020]
- , *The UK-Swiss Tax Agreement: Doomed to Fail. Why the Deal Will Raise Little, and May Be Revenue-Negative for the UK*, 21 October 2011 <[www.taxjustice.net/cms/upload/pdf/TJN\\_1110\\_UK-Swiss\\_master.pdf](http://www.taxjustice.net/cms/upload/pdf/TJN_1110_UK-Swiss_master.pdf)> [accessed 22 January 2020]
- US Bureau for International Narcotics and Law, and Enforcement Affairs, *International Narcotics Control Strategy Report, Volume II: Money Laundering and Financial Crimes* (March 2016) <<https://2009-2017.state.gov/documents/organization/253983.pdf>> [accessed 29 January 2020]

---

<sup>1</sup> 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 2020 takes into account the results of the new assessments. The old recommendations can be viewed at: Financial Action Task Force, *Financial Action Task Force on Money Laundering. The Forty Recommendations.*, 2003 <<http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf>> [accessed 29 January 2020].; the new recommendations are available at: Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations (2012 - Updated 2019)* (Paris, June 2019) <<https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>> [accessed 29 January 2020].

<sup>2</sup> Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations (2012 - Updated 2019)*. Also see footnote above.

<sup>3</sup> 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.

<sup>4</sup> Financial Action Task Force, *Financial Action Task Force on Money Laundering. The Forty Recommendations*. Also see footnote above.

<sup>5</sup> 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.

<sup>6</sup> While we would have liked to include the data from the 2019 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.

<sup>7</sup> Financial institutions in some jurisdictions are required to report on large transactions above a certain threshold (INCSR, 2019: 10). Threshold based disclosures are used in addition to suspicious transactions reporting, and apply regardless of the amount involved. They can be useful, mainly because unlike suspicious transactions reporting, they are not subjective, and thus their interpretation may not vary from one country to the other. See European Parliamentary Research Service - EPRS, 'Fighting Tax Crimes: Ex-Post Evaluation of the Cooperation between Financial Intelligence Units' (2017) <[http://www.europarl.europa.eu/RegData/etudes/STUD/2017/598603/EPRS\\_STU\(2017\)598603\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2017/598603/EPRS_STU(2017)598603_EN.pdf)> [accessed 29 January 2020].

<sup>8</sup> The information is presented in the table on pages 40-50 under the column "Report Large Transactions", in: US Bureau for International Narcotics and Law and Enforcement Affairs, *International Narcotics Control Strategy Report, Volume II: Money Laundering and Financial Crimes* (March 2016) <<https://2009-2017.state.gov/documents/organization/253983.pdf>> [accessed 29 January 2020].

<sup>9</sup> 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.

<sup>10</sup> 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.

<sup>11</sup> 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).

<sup>12</sup> 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.).

<sup>13</sup> 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.

<sup>14</sup> Tax Justice Network, ‘Financial Secrecy Index 2020 Questionnaire’ <[https://www.financialsecrecyindex.com/PDF/FSI2020\\_Questionnaire-MOF-NAO.xlsx](https://www.financialsecrecyindex.com/PDF/FSI2020_Questionnaire-MOF-NAO.xlsx)> [accessed 29 January 2020].

<sup>15</sup> 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.

<sup>16</sup> 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.

<sup>17</sup> Tax Justice Network, ‘Tax Information Exchange Arrangements’, 2009 <[http://www.taxjustice.net/cms/upload/pdf/Tax\\_Information\\_Exchange\\_Arrangements.pdf](http://www.taxjustice.net/cms/upload/pdf/Tax_Information_Exchange_Arrangements.pdf)> [accessed 24 January 2020].

<sup>18</sup> Markus Meinzer, ‘Automatic Exchange of Information as the New Global Standard: The End of (Offshore Tax Evasion) History?’, *SSRN Electronic Journal*, 2017 <<http://www.ssrn.com/abstract=2924650>> [accessed 29 January 2020].

<sup>19</sup> Tax Justice Network, ‘Key Financial Secrecy Indicator 18: Automatic Information Exchange’, 2020 <<http://www.financialsecrecyindex.com/PDF/18-Automatic-Info-Exchange.pdf>> [accessed 29 January 2020].

<sup>20</sup> See page 17, in: Markus Meinzer, *Steueroase Deutschland: Warum Bei Uns Viele Reiche Keine Steuern Zahlen* (Munich, 2015).

<sup>21</sup> Fowler, Naomi, ‘Whistleblower Rudolf Elmer: Legal Opinion on Latest Ruling’, 2019 <<https://www.taxjustice.net/2019/06/04/whistleblower-rudolf-elmer-legal-opinion-on-latest-ruling/>, <https://www.taxjustice.net/2019/06/04/whistleblower-rudolf-elmer-legal-opinion-on-latest-ruling/>> [accessed 29 January 2020]. Der Spiegel, ‘Schweizer Geheimdienst Sammelte Informationen Über Deutsche Steuerfahnder’, 2 May 2017 <<https://www.spiegel.de/wirtschaft/soziales/schweizer-geheimdienst-sammelte-informationen-ueber-deutsche-steuerfahnder-a-1145703.html>> [accessed 29 January 2020].

<sup>22</sup> Bastian Brinkmann, Obermaier, Frederik and Bastian Obermayer, ‘Wie Einfache Bürger Billige Dienste Für Offshore-Kunden Leisten’, *Süddeutsche.De* (18 April 2016) <<http://www.sueddeutsche.de/politik/mittelamerika-leticia-und-die->

---

briefkasten-oma-1.2954968> [accessed 29 January 2020].; Tax Justice Network, *The UK-Swiss Tax Agreement: Doomed to Fail. Why the Deal Will Raise Little, and May Be Revenue-Negative for the UK*, 21 October 2011  
<[www.taxjustice.net/cms/upload/pdf/TJN\\_1110\\_UK-Swiss\\_master.pdf](http://www.taxjustice.net/cms/upload/pdf/TJN_1110_UK-Swiss_master.pdf)>  
[accessed 22 January 2020].