HUMAN RIGHTS AND MONEY LAUNDERING: A COMPARATIVE ANALYSIS OF THE SUSPICIOUS TRANSACTION REPORTS REGIME FROM A PERSONAL DATA PROTECTION RIGHTS PERSPECTIVE

MUSTAFA AKGUN

HUMAN RIGHTS AND MONEY LAUNDERING: A COMPARATIVE ANALYSIS OF THE SUSPICIOUS TRANSACTION REPORTS REGIME FROM A PERSONAL DATA PROTECTION RIGHTS PERSPECTIVE

MUSTAFA AKGÜN

A letter believed to be written by Benjamin Franklin in 1755 on behalf of the Pennsylvania Assembly noted that:

> Those who would give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety.

While the 'essential liberty' in the letter was referring to the colonies' right of self-governance, this statement is often quoted in surveillance and privacy-related pieces. This is normal because this quote perfectly explains the relationship between the privacy rights of individuals and the surveillance powers of law enforcement authorities.

The war against money laundering and underlying offences relies on information supplied by the financial industry filing their Suspicious Transaction Reports. The effectiveness of the Suspicious Transaction Reports regime is subject to a vivid debate. One problem of the reporting regime in most countries is the overwhelming number of unwarranted defensive reports bankers make. A significant problem leading reporters to make unwarranted disclosures is Anti-Money Laundering laws in breach of banking clients' privacy rights.

This thesis defends that re-designing the Suspicious Transaction Reports regime in compliance with information privacy laws will increase the success in the fight against economic crime, criminal money and money laundering. Hence, it defends that those who fight for information privacy rights will also gain security.

HUMAN RIGHTS AND MONEY LAUNDERING: A COMPARATIVE ANALYSIS OF THE SUSPICIOUS TRANSACTION REPORTS REGIME FROM A PERSONAL DATA PROTECTION RIGHTS PERSPECTIVE

In One Volume

Mustafa Akgün

Submitted for the degree of Doctor of Philosophy

Durham Law School

St Mary's College

Durham University

August 2021

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I would like to express my thanks to everyone who supported me throughout this research project. I would also like to mention by name some of them here.

First of all, I would like to say a special thank you to my supervisors Prof. Deryck Beyleveld and Prof. Helen Fenwick. Without their support, guidance and overall insights in this field, I would not have been able to complete this research. I will miss our meetings with Deryck starting at 9 am and not finishing before the lunch time.

I would like to say a big thank you to everyone at Durham Law School I have had a cup of coffee or tea with.

I would like to thank Dr Tom Fisher and Ailidh Callander from Privacy International for their consistent support during the running of this project.

I would also like to say thank you to my good friends in Durham, Beyza Ustun, David Reay, Fawaz Al-Khateeb, Helen Rodway, Kershwyn Basuday, Kristiyan Stoyanov, Mavis Wang, Suleyman Yildirim and Zekiye Goz (ordered alphabetically).

I would like to express my gratitude to the Turkish Ministry of Education for granting me a scholarship.

Lastly, from the bottom of my heart I would like to say thank you to my parents Ziya and Muserref Akgun and my sister Sumeyye Akgun.

CHAPTER 1: INTRODUCTION

This introductory chapter involves two sub-chapters. The following sub-chapter 1.I presents the research questions on which this thesis focuses and explains the reason why those questions are chosen. Sub-chapter 1.III summarises the arguments defended in this thesis.

1.II. Research questions

This thesis investigates Anti-Money Laundering (AML) laws requiring and permitting banks to make Suspicious Transaction Reports (STRs) from the perspective of banking clients' right to the protection of personal data, focusing on the following set of questions:

(1) To what extent and under what conditions do AML laws require and permit banks to make STRs?

(1a) To what extent and under what conditions does the Financial Action Task Force (FATF), in its recommendations 3, 20 and 21, advise countries to require and permit banks to make STRs?

(1b) To what extent and under what conditions do English AML laws require and permit banks to make Suspicious Activity Reports (SARs[1])?

(1c) To what extent and under what conditions do Swiss AML laws require and permit banks to make SARs?

(2) What are the data protection rules with which AML laws requiring and permitting banks to make STRs should comply?

(2a) What are the data protection rules with which the FATF's recommendations 20 and 21 should comply?

(2b) What are the data protection norms with which English AML laws requiring and permitting banks to make SARs should comply?

(2c) What are the data protection norms with which Swiss AML laws requiring and permitting banks to make SARs should comply?

(3) What is the reason why countries should establish a system where banks share their money-laundering suspicions with competent law enforcement agencies?

(4) To what extent does the STRs regime comply with applicable data privacy rules?

(4a) To what extent do the FATF recommendations 20 and 21 comply with information privacy laws to which recommendation 2 referred?

(4b) To what extent do English AML laws requiring and permitting banks to make SARs comply with applicable data privacy rules?

[1] In relation to the difference between STRs and SAR, see page 17 in chapter 2.

(4c) To what extent do Swiss AML laws requiring and permitting banks to make SARs comply with applicable data privacy rules?

(5) What is the way in which AML rules that breach applicable data privacy standards affect the STRs regime's effectiveness?

1.II.A. What is the reason why this thesis investigates the STRs rules applying to the banks?

The powers and responsibility of police authorities have long been a popular research topic. The 20th century witnessed many radical changes, one of which is the appearance of so-called policeman duties and privileges of private entities.[2] This fundamental change drives legal scholars to investigate a new issue: the powers and responsibility of so-called private policemen.

AML laws made professionals (i.e. banks, non-bank financial institutions and designated non-financial businesses and professions) the private policemen of the financial sphere.[3] First, private entities are expected to inform competent public authorities by making an STR where they know or suspect that their client's funds constitute or represent criminal money.[4] Second, they are expected to know their clients by undertaking customer due diligence and record-keeping measures.[5] Third, they are expected to analyse and understand the money laundering risk to which they are exposed and take AML measures in a risk-sensitive manner.[6]

The effectiveness of the STRs regime, discussed in several national and European reports published in the last five years, is subject to a vivid debate.[7] This thesis focuses on the STRs related AML laws.

[2] Eg. Anti-Money Laundering/Counter-Terrorist Financing laws which made professionals the private policemen of the financial sphere, and Anti-terrorism laws imposing upon internet domain providers duty to play a policeman role in the fight against terrorist propaganda. For further examples, see M. Akgun, 'La réforme française du 13 Novembre 2014 sur le blocage administratif des sites internet provoquant au terrorisme ou en faisant l'apologie' [2016] 25(7) TAAD 223, 228-234.

[3] J. Wadsley, 'Money laundering: professionals as policemen' (1994) Conv. 275, 275-277.

[4] Recommendations 20 and 23. FATF (2012-2020), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, 19, <www.fatf-gafi.org/recommendations.html> 10 June 2021.

[5] Recommendations 10-19, and 22. FATF (n,4), 14-19. See pages 24-28.

[6] Recommendation 1. FATF (n,4), 10. FATF, 'Guidance for A Risk-based approach - the banking sector' October 2014, 6 <http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf> 10 June 2021. See pages 21-23.

[7] Eg. Europol analysed the success of the STRs regime in its 2017 report. Europol Report, 'From suspicion to action: Converting financial intelligence into greater operational impact' (2017) <https://www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact> 1 June 2021. The Law Commission of England and Wales called for a reform in its' 2019 SARs regime report. Law Commission, *Anti-money laundering: the SARs regime* (Law Com No 384, 2019).

AML laws impose upon banks, non-bank financial institutions and designated non-financial businesses and professions duty of making STRs.[8] The extent to which one is permitted and required to share their money-laundering suspicions with competent public authorities depends on the business in which they are working. For instance, bankers' duty to report is not the same as lawyers and casinos.[9] This thesis focuses on the STRs regime that applies to banks because banks are the primary source of the STRs. In its 2017 report, Europol demonstrated that the primary source of STRs between 2006 and 2014 in all the EU countries was the banks and credit institutions.[10] English and Swiss Financial Intelligence Units' annual reports also show that banks are well ahead of other institutions according to the number of reports they made. From 2014 to 2020, banks made 80% of the SARs in the UK, while this figure goes up to 89% in Switzerland (see charts 1 and 2).[11]

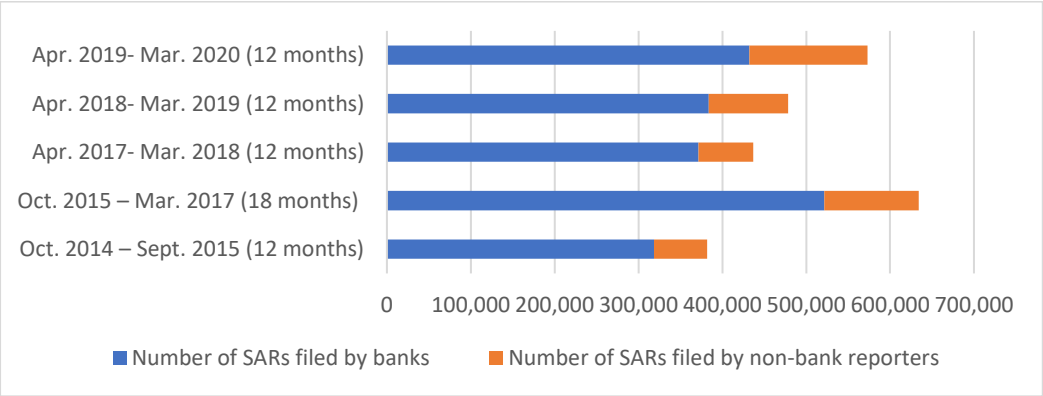


Chart 1: Number of SARs made by banks and other private persons in the UK from October 2014 to March 2020[12]

[8] Recommendations 20 and 23. FATF (n,4), 19-21.
[9] See Recommendations 20, 21 and 23, FATF (n,4), 19-21.
[10] Europol (n,7), 14.
[11] Banks produced 80% of the SAR in the UK from October 2014 to March 2020. For further details, see chart 1. Banks produced 89% of the SAR in Switzerland from January 2015 to December 2020. For further details, see chart 2. For further statistics in relation to the SARs filed in the EU member states, see Europol (n,7), 14.
[12] This chart was prepared by using information provided in the UKFIU's Annual reports 2020, 2019, 2018, 2017, 2015. See National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2020', (2020), 9; National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2019', (2019), 8; National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2018', (2018), 6; National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2017', (2017), 12; and National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2015', (2015), 9.

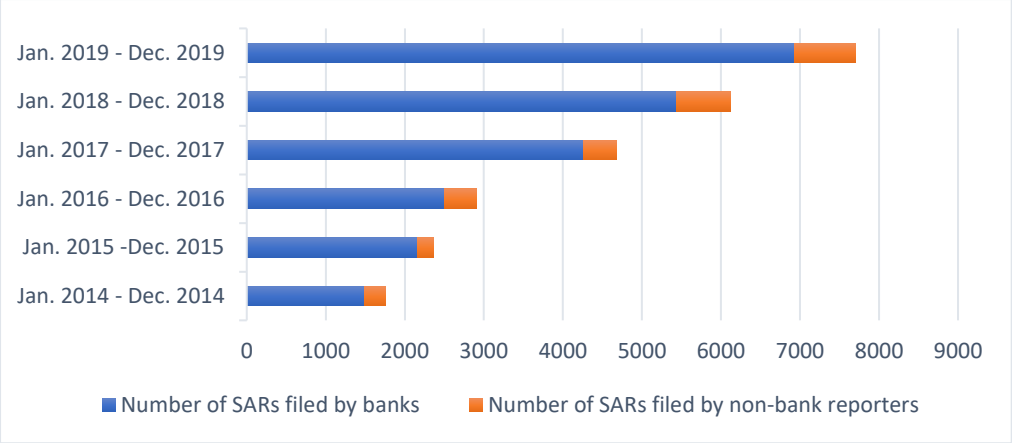


Chart 2: Number of SARs made by banks and other private persons in Switzerland from January 2014 to December 2019.[13]

Banks may lose their existing and prospective clients if the people learn that it shared its client's financial secrets with a third party.[14] Banks are profit-oriented entities, and they naturally wish to protect their financial attractiveness. Therefore, banks have never been very keen on informing public authorities of their client's unusual or suspicious transactions. Lawmakers, therefore, took measures to convince banks to share their money-laundering suspicions with competent public authorities. First, AML laws imposed upon banks and their staff duty to produce STRs.[15] Second, lawmakers took measures to protect reporters' legal and financial interests. For instance, the reporters are protected from criminal and civil liability for breach of any restriction on disclosure of information where they acted in good faith.[16] Moreover, the reported banking client's right to access personal data is limited. This thesis investigates AML laws requiring and permitting banks to make STRs.

[13] This chart was prepared by using information provided in the MROS's Annual reports 2019, 2018, 2017, 2016 and 2015. See Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2019', (Avril 2020), 7; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2018', (Avril 2019), 8; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2017', (Avril 2018), 8; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2016', (Avril 2017), 8; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2015', (Avril 2016), 7.
[14] See pages 37-37 and 64-66 in chapter 2.
[15] Recommendation 20. FATF (n,4), 19.
[16] See Recommendation 21. FATF (n,4), 19.

1.II.B. What is the reason why this thesis investigates the STRs regime from a personal data protection rights perspective?

Several international human rights instruments require their signatories to protect individuals' right to the protection of personal data.[17] Many countries, including the UK and Switzerland,[18] amended their existing laws and adopted new acts to give effect to the right to the protection of personal data.[19] The FATF, which sets universally recognised international standards for combating money laundering, and other related threats to the integrity of the international financial system, has also integrated data protection and privacy rules.[20] Indeed, the FATF's recommendation 2, as amended in February 2018, advises countries to ensure AML measures compatibility with data protection and privacy rules.[21]

English and Swiss laws recognised data subject's *prima facie* exclusive control rights over their personal data. A banker's filing of an STR often interferes with the reported client's *prima facie* control rights over his personal data. Data subject's relevant rights can be limited under certain conditions. The STRs regime should comply with the rules relating to the restriction of personal data protection rights.

As explained above, the STRs regime should comply with some data protection rules. However, few studies examined the STRs regime from a data protection rights perspective.[22] This is for two reasons.

---

[17] Eg. the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108); the Charter of Fundamental Rights of the European Union; and OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

[18] See UK Data Protection Act 2018; Swiss Federal Act on Data Protection 1992 and Swiss revised-Data Protection Act 2020.

[19] By the end of 2018, there are more than 130 countries that have enacted data privacy laws. See G Greenleaf, 'Global Data Privacy Laws 2019: 132 National Laws & Many Bills' (2019) 157 Privacy Laws & Business International Report 14, 14-18.

[20] Recommendation 2, FATF (n,4), 10.

[21] Ibid.

[22] While the effectiveness of the SARs regime has been discussed, the SAR's regime's compliance with information privacy laws was not extensively investigated in the Europol and Law Commission reports. See Europol (n,7); and Law Commission (n,7).
The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism submitted to the General Assembly a report where the FATF's countering terrorist financing standards were investigated from a Human Rights perspective. See UN, A/74/335 "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism" <https://undocs.org/A/74/335> 10 June 2021). Following this report, Privacy International in London produced a report in 2019 on the application of the FATF standards and its' influence on individuals' privacy rights. (Privacy International, 'How financial surveillance in the name of counter-terrorism fuels social exclusion' (2019), <https://www.privacyinternational.org/long-read/3257/how-financial-surveillance-name-counter-terrorism-fuels-social-exclusion> 10 June 2021).
Greenleaf and Tyree investigated the relation between bankers' AML duties and data protection laws in G Greenleaf and A Tyree, Bankers' Duties and Data Privacy Principles: Global Trends and Asia-Pacific Comparisons' in S Booysen and D Neo (eds) *Can Banks Still Keep a Secret?: Bank Secrecy in Financial Centres Around the World* (Cambridge University Press 2017). However, this book chapter was focused on the regulations in Asia-Pasific countries.
Banks' and their staff's role in the fight against criminal money was investigated from a privacy rights perspective by Janet Ulph in J Ulph, *Commercial Fraud: Civil Liability, Human Rights and Money Laundering* (OUP 2006).
Stokes investigated banks' duty of suspicious activity reporting from a Human Rights perspective in R Stokes, 'The banker's duty of confidentiality, money laundering and the Human Rights Act' (2007) 9 (3) J.B.L. 525 and

First, protecting banking clients' information privacy rights and fighting against money laundering were long conceived as two conflicting aims.[23] The fact that the right to privacy is misunderstood or misused by some has also helped disseminate this misconception.[24] Second, data protection laws are relatively new.[25] Most of the authors who investigated the STRs regime from an information privacy rights perspective focused on the balance between banking institutions' AML duties, on the one hand, and banks' duty of confidentiality, on the other hand. However, they did not give sufficient weight to data protection laws. Data protection laws, compared to the law of confidence, provide data subjects with more robust protection.[26] By analysing the above-listed questions, this thesis aims to fill the gap in the literature.

1.II.C What is the reason why this thesis employs a comparative law method?

This thesis employs a comparative law method. Because the FATF set non-binding global standards to protect the banking industry from the threat of money laundering, this thesis takes the FATF Recommendations as a starting point.[27] The FATF formulated its recommendations in a way that is open to different interpretations. This thesis investigates English and Swiss laws to see various interpretations of these recommendations. Hence, relevant FATF Recommendations and their application in English and Swiss AML laws are at the centre of this research.

1.II.C.1. The FATF recommendations that established the international standards

This thesis takes the FATF Recommendations as a starting point because the FATF has set universally recognised international standards for combating money laundering and other related threats to the integrity of the international financial system.[28]

---

in R Stokes, 'The Banker's Duty of Confidentiality' (PhD thesis, University of Liverpool, 2005), Ch. 4. See also R. Cranston et all, *Principles of Banking Law* (3rd ed, OUP 2018), Ch. 9, where the conflict between bankers' AML duties and bankers' duty of confidentiality was investigated.

[23] The fact that OECD started a process that they named "The era of bank secrecy is over" reflects this approach. See 'The Era of Bank Secrecy is over; The G20/OECD Process is Delivering Results' (26 October 2011 OECD) <https://www.oecd.org/ctp/exchange-of-tax-information/48996146.pdf> 10 June 2021.

[24] A recent example where privacy rights concept seems to be used as a cover for an economic profit orientated project may be the Swiss federal popular initiative «Oui à la protection de la sphère privée» (Yes to the protection of the private sphere), where the petitioners opposed limitation of bank secrecy in tax matters for the sake of privacy rights. See « Arrêté fédéral relatif à l'initiative populaire «Oui à la protection de la sphère privée» (Projet) », FF 2015 6467 for the Federal Bill relating to the popular initiative "Yes to the protection of the private sphere" and «Initiative populaire fédérale «Oui à la protection de la sphère privée». Retrait», FF 2018 212 for withdrawal of the Bill.

[25] O Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015), 87.

[26] For further information, see pages 58-101 in chapter 3.

[27] FATF (n,4), 7.

[28] Ibid.

Money launderers are heavily misusing banking products and services while this threat is globally well-known since, at least, the Chiasso affair of the 1970s.[29] Countries' failure in protecting the international financial system from the money laundering threat has several financial, political and legal reasons, one of which is that some countries' failure to place banks and their staff in a proper position in the fight against money laundering.[30] A legal system's inability to put banks in an appropriate place in the fight against money laundering may lead to the failure of that legal systems' AML policy. Failure of one country may lead to a global failure because "global safeguards to combat money laundering […] are only as strong as the jurisdiction with the weakest measures".[31] This is because of the global nature of the international financial system where the offence of money laundering takes place. The state borders are currently no stronger than beaded curtains against offenders involved in criminal offences takes place in the international financial system (eg. money laundering, terrorist financing and international tax evasion[32]), or on online platforms (eg. terrorist propaganda on online platforms,[33] online image-based sexual abuse[34]). Different stages of the offence of money laundering can occur in different countries that are part of the international financial system, and hiding one stage in one country may help criminals hide the criminal money and/or some criminal authors, if not the whole criminal process. Hence, because funds can freely, quickly, and safely move worldwide, no sub-part of the international financial system (including independent countries and regional unions such as the EU) can successfully fight against criminal money without international cooperation.

The transnational nature of money laundering offences led to the adoption of AML rules, particularly rules relating to the financial institutions' duties and privileges, which transcend nation-states. Transnational law can emerge in two ways at the public level. States and intergovernmental organisations can produce transnational law with binding or non-binding rules.[35] The FATF is an inter-governmental body having 39 members established in 1989.[36] Since 1990, it makes non-binding recommendations and updates these recommendations "to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist

[29] For further details, see pages 149-159 in chapter 4.
[30] Europol (n,7),12; F Hobson, 'Introduction: Banks and Money Laundering' in W Blair and R Brent (eds) *Banks and Financial Crime: The International Law of Tainted Money* (OUP 2008), 15.
[31] FATF website, 'High-risk and other monitored jurisdictions', <http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/more/more-on-high-risk-and-non-cooperative-jurisdictions.html?hf=10&b=0&s=desc(fatf_releasedate)> 10 June 2021.
[32] M. Zwick, *Banking Secrecy and Money Laundering* (Promoculture sarl 2003), 17.
[33] Akgun (n1) 229.
[34] Another famous example of the crimes against which one country's failure leads a global failure is the online image based abuse of minors. For instance, the impact analysis report of the French act 2011-267 (ie. loi nº 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure) has shown that 50% of the minor pornography content on internet had been uploaded by a Russian host website until 2007. See J. Cattan, « Le droit et les communications électroniques », (PhD Thesis, Aix-en-Provence 2012), 513.
[35] M. Siems, *Comparative Law* (Cambridge University Press: 2014), 249.
[36] FATF (n4) 7.

financing and other related threats to the integrity of the international financial system".[37] As a policy-making body, the FATF has reached global success. Indeed, its recommendations have been endorsed by over 180 countries.[38] The FATF's recommendations are taken as a strong example of influential international soft law in comparative law literature.[39] Because of their success in influencing national laws worldwide, this thesis puts the FATF Recommendations to the centre.

1.II.C.2. Why does this thesis focus on the FATF Recommendations' application in English and Swiss laws?

The FATF played a prominent role in the appearance and evolution of the rules that determine banks' role in the fight against economic crime, criminal money and money laundering. Whilst, national laws are still important for two reasons. First, the FATF standards are not legally binding.[40] Second, the FATF Recommendations are general standards whose precise application needs to be determined by national authorities.[41] Therefore, these recommendations have been adopted into national laws in a number of significantly different ways.

To critically analyse banking institutions' role in the fight against money laundering, this thesis investigates not only broad standards recommended by the FATF but also their application in national laws. A comprehensive study needs to examine the application of these recommendations in more than one jurisdiction to identify different applications of the relevant broad standards. Therefore, this thesis compares English and Swiss AML laws.

The UK and Switzerland are chosen as comparison states due to two reasons. First, a comparison of these two legal systems permits this thesis to identify the FATF Recommendations' different applications. English and Swiss AML laws represent two different approaches concerning the balance between banking clients' information privacy rights and banks' AML duties, while they both are in above-average compliance with the FATF's recommendations. Second, a UK- Switzerland comparison may give this thesis a strong impact capacity. This is because the UK and Switzerland represent two prominent financial centres influential in the development of relevant international banking and AML

[37] Ibid.
[38] Ibid, 6,7.
[39] Siems (n,35), 253; N W Turner, 'The Financial Action Task Force: International Regulatory Convergence through Soft Law' (2014-2015) 59 N.Y. L. Sch. L. Rev. 547, 555.
[40] While the recommendations are not legally binding, non-compliance with the FATF recommendations may have significant financial adverse effect on blacklisted countries. In relation to the FATF blacklists' financial effects, see. K Eggenberger, 'When is blacklisting effective? Stigma, sanctions and legitimacy: the reputational and financial costs of being blacklisted" [2018] 25(4) *Review of International Political Economy* 483, 490; and Privacy International (n,22); cf. O Balakina, A D'Andrea and D Masciandaro, 'Bank secrecy in offshore centres and capital flows: Does blacklisting matter?' [January 2017] 32 *Review of Financial Economics* 30, 31.
[41] FATF (n,4) 6.

standards.[42] Hence, this thesis compares applicable English and Swiss laws since this comparison facilitates elaborating a coherent and comprehensive analysis that may have a substantial impact capacity.

1.II.C.2.a. UK-Switzerland comparison permits this thesis to identify different applications of the FATF standards.

This thesis employs a comparative law method to identify different applications of the FATF standards. Therefore, comparison states must be chosen amongst those countries whose AML laws comply with these standards.[43] Both English and Swiss AML laws are in above-average compliance with the FATF Recommendations. According to the Mutual Evaluation Report relating to the implementation of AML/CTF standards in Switzerland undertaken by the FATF in 2016 and the 3rd Enhanced Follow-up Report & Technical Compliance Re-Rating report published in January 2020, Swiss law is "compliant" or "largely compliant" with 35 of the 40 Recommendations.[44] The last FATF Mutual Evaluation Report relating to the implementation of AML/CTF standards in the UK in 2018 concluded that English law was "compliant" or "largely compliant" with 38 of the 40 Recommendations.[45] Hence, English and

[42] Siems (n,35), 32.

[43] Comparison states must show some similarities in some basic aspects to produce a coherent comparison. These basic similarities depend on the subject and aim of the comparison. See O Pfersmann 'Le droit comparé comme interprétation et comme théorie du droit' (2001) 53(2) *Revue internationale de droit comparé* 278, 282-285 for further explanation of the principles to be applied in choosing comparison states.

[44] In the Mutual Evaluation Report relating to the implementation of AML/CTF standards in Switzerland undertaken by the FATF in 2016, Swiss AML/CTF laws were deemed compliant with the Recommendations 9 (financial institution secrecy laws), 11 (record keeping), 14 (Money or value transfer services) and 29 (Financial intelligence units); largely compliant with the Recommendations 1 (assessing risk & applying risk-based approach), 12 (Politically exposed persons), 13 (Correspondent banking), 17 (Reliance on third parties), 18 (Internal controls and foreign branches and subsidiaries), 20 (Reporting of Suspicious transactions), 21 (Tipping-off and confidentiality), 26 (Regulation and supervision of financial institutions), 27 (Powers of supervision) and 34 (Guidance and feedback); partially compliant with the Recommendations 10 (Customer due diligence) and 16 (Wire transfers). See FATF (2016), Anti-money laundering and counter-terrorist financing measures - Switzerland, Fourth Round Mutual Evaluation Report, FATF, Paris, France, 11 <www.fatf-gafi.org/publications/mutualevaluations/documents/mer-switzerland-2016.html> 10 June 2021. In the 3rd Enhanced Follow-up Report & Technical Compliance Re-Rating report published in January 2020, Swiss law has been re-rated in relation to Recommendations 8 (Largely Compliant), 16 (Largely Compliant), 19 (Compliant) and 33 (Compliant). FATF (2020), Anti-money laundering and counter-terrorist financing measures - Switzerland, Enhanced Follow-up Report & 2nd Technical Compliance Re-Rating, FATF, Paris, 2 <http://www.fatf-gafi.org/publications/mutualevaluations/documents/fur-switzerland-2020.html>.

[45] English AML/CTF laws were deemed compliant with the Recommendations 9 (financial institution secrecy laws), 11 (record keeping), 12 (Politically exposed persons), 14 (Money or value transfer services), 20 (Reporting of Suspicious transactions), 21 (Tipping-off and confidentiality), 26 (Regulation and supervision of financial institutions), 27 (Powers of supervision) and 34 (Guidance and feedback); largely compliant with the Recommendations 1 (assessing risk & applying risk-based approach), 17 (Reliance on third parties) and 18 (Internal controls and foreign branches and subsidiaries); and partially compliant with the Recommendations 13 (Correspondent banking) and 29 (Financial intelligence units). See FATF (2018), Anti-money laundering and counter-terrorist financing measures – United Kingdom, Fourth Round Mutual Evaluation Report, FATF, Paris, France, 14, <http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-kingdom2018.html> 10 June 2021

Swiss AML laws largely reflect the FATF standards. Comparing these two legal systems may lead to an accurate and coherent comparative analysis.

AML laws may contradict information privacy laws. The FATF, in its recommendation 9, advised countries to "ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations". In February 2018, the FATF revised its' recommendation 2 and advised countries to ensure the compatibility of AML "requirements with Data Protection and Privacy rules and other similar provisions". [46] Interpretive Note to Recommendation 2 does not provide further explanation in relation to the effect of the second sentence of paragraph 2 of recommendation 2 on AML rules. Moreover, the FATF rarely refers to privacy and data protection rules, even in post-2018 mutual evaluation reports.[47] Consequently, while some FATF compliant countries give preponderant importance to privacy and confidentiality rights, some prefer relatively aggressive AML measures. To consider different applications of the relevant FATF Recommendations, countries that represent different approaches should be chosen to be compared.[48]

This thesis employs comparative law to identify different interpretations of the FATF standards. Therefore, it focuses on English and Swiss laws. The UK, ranked 23rd and 12th in the 2018[49] and 2020[50] Financial Secrecy Indexes after most major financial centres,[51] has privileged strict AML measures. The FATF officials underlined in 2018 that "[t]he UK routinely and aggressively identifies, pursues and prioritises ML investigations and prosecutions".[52] Switzerland, ranked 1st and 3rd in the 2018[53] and 2020 Financial Secrecy Index,[54] is famous for its' bank secrecy laws. The 2020 Financial Secrecy Index report underlined that "Switzerland is the grandfather of the world's tax havens, .. and one of the world's biggest secrecy jurisdictions..."[55] Similarly, 2016 FATF Mutual evaluation report recognised the importance of bank secrecy in Switzerland as follows: "[Switzerland] is an extremely attractive financial centre. Banking secrecy also contributed for a long time as a factor in this attraction."[56]

---

[46] FATF Recommendation 2, *National cooperation and coordination* amanded in February 2018, FATF (n,4), 10.

[47] For instance, see FATF (2020) (n43); FATF (2018) (n44).

[48] In relation to choice of comparison states, see : Pfersmann (n,43), 278 ; and M. Izorche « Propositions methodologiques pour la comparaison » (2001) 53(2) Revue internationale de droit compare 289.

[49] Tax Justice Network, 'Financial Secrecy Index 2018 - Narrative Report on the United Kingdom', 2018, 1, <http://www.financialsecrecyindex.com/PDF/UnitedKingdom.pdf> 10 June 2021.

[50] Tax Justice Network, 'Financial Secrecy Index 2020 - Narrative Report on the United Kingdom' , 2020, 1 <https://fsi.taxjustice.net/PDF/UnitedKingdom.pdf> .

[51] See "Financial Secrecy Index - 2018 Results" in the tax justice network's website, <https://www.financialsecrecyindex.com/introduction/fsi-2018-results> 10 June 2021 and "Financial Secrecy Index – 2020 Results" in the tax justice network's website, <https://fsi.taxjustice.net/en/introduction/fsi-results> 10 June 2021.

[52]FATF (2018) (n45) 3.

[53] Tax Justice Network "Financial Secrecy Index 2018 - Narrative Report on Switzerland", 2018, <http://www.financialsecrecyindex.com/PDF/Switzerland.pdf> 10 June 2021.

[54] Tax Justice Network, "Financial Secrecy Index 2020 - Narrative Report on Switzerland", 2020, <https://fsi.taxjustice.net/PDF/Switzerland.pdf>10 June 2021.

[55] Ibid.

[56] See FATF (2016) (n,43), 19.

Therefore, a UK - Switzerland comparison enables this thesis to identify relevant FATF Recommendations' different applications.

Besides, comparing legal position in the UK, a leading common law country, and Switzerland, a civil law country where private law has largely been influenced by the pioneer civil law jurisdictions France and Germany,[57] enables this thesis to reveal different approaches adopted in these two very close but still different legal families.[58]

1.II.C.2.b. UK-Switzerland comparison may help this thesis have a substantial impact capacity.

Comparing the SARs regime accepted in English and Swiss AML laws enhances the impact capacity of this thesis. The UK and Switzerland are two prominent financial systems whose banking sectors are exposed to a high risk of money laundering,[59] and they play an essential role in the development of international AML standards. The UK is one of the members of the G7, by whose 1989 summit the FATF was established,[60] while Switzerland is one of the 39 members of the FATF.

The UK and Switzerland represent two major global financial centres with prominent banking sectors. Indeed, the UK and Switzerland represent the second and eighth largest global financial centres, respectively.[61] Moreover, the UK and Switzerland remain the world's 1st and 3rd leading net exporters of financial services, respectively.[62] Banking constitutes the most prominent financial business in both countries.[63] Besides, the UK and Switzerland consolidated banking assets are the 1st and 5th largest in

[57] P G Picht and G Studen, "Civil Law" in D Hurlimann and M Thommen (eds.), *Introduction to Swiss Law – Volume 2* (Carl Grossmann Publishers 2018), 273. Prior to the Federal Code of Obligations 1881, private law in Switzerland was enacted at cantonal levels. While some cantonal laws (eg. Genève, Vaud, Neuchâtel, Tessin and Jura bernois) were influenced by the Napoleonic Code (the French Civil Code 1804), some others (eg. Berne, Soleure, Argovie, Lucerne) were influenced by the General Civil Code of Austria 1811 (ABGB 1811). B. Schnyder, Code Civil (CC) in Dictionnaire Historique de la Suisse, version 18.11.2014 <http://www.hls-dhs-dss.ch/textes/f/F30734.php 1> 10 June 2021.

[58] For a broader discussion of comparing common law and civil law legal systems, see Siems (n35), Ch 3.

[59] "The UK faces significant ML risks from overseas, in particular from other global financial centres (including some of its Overseas Territories and Crown Dependencies), due to its position as a major global financial centre and the world's largest centre for cross-border banking." FATF (2018) (n,44), 18. With regard to Switzerland, see FATF (2016) (n,43) 3.

[60] 'Economic Declaration', Paris, 16 July 1989. <http://www.g8.utoronto.ca/summit/1989paris/communique/index.html> 10 June 2021

[61] M Yeandle and M Wardle, 'The Global Financial Centres Index 25 March 2019', 4 <https://www.longfinance.net/media/documents/GFCI_25_Report.pdf> 10 June 2021.

[62] The City UK,"Key facts about the UK as an international financial centre 2018" (The City UK, October 2018) https://www.thecityuk.com/assets/2018/Reports-PDF/94053cfc7b/Key-facts-about-the-UK-as-an-international-financial-centre-2018.pdf at 3

[63] For the UK, see FATF (2018), (n44), 9. For Switzerland: FATF (2016) (n43), 18.

Europe, respectively.[64] Furthermore, their banking sectors have a strong international dimension.[65] While the UK is the world's largest centre for cross-border banking, Switzerland is the global leader for cross-border private banking.[66] The relevant FATF reports established that both English and Swiss financial systems are attractive for laundering assets derived from offences that are mostly committed abroad.[67] Therefore, money launderers have long threatened the UK and Switzerland. Consequently, the UK and Switzerland played an essential role in the development of the international AML standards.

1.II.C.2.c. Limitation

Switzerland consists of French-, German-, Italian, and Romansh- speaking cantons, and these four languages are the official languages of the Confederation. However, the author of this thesis speaks only one of these languages, French. Accordingly, Swiss law is investigated with reading through French- and English- speaking literature only. Moreover, when cantonal laws need to be specified, this research focuses on the French-speaking cantons, particularly Geneva, the birthplace and capital of international asset management.[68]

1.II. Arguments

Summary. A letter believed to be written by Benjamin Franklin in 1755 on behalf of the Pennsylvania Assembly noted that:[69]

> Those who would give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety.

While the 'essential liberty' in the letter was referring to the colonies' right to self-governance,[70] this statement is often quoted in surveillance and privacy-related pieces. This is normal because this quote perfectly explains the relationship between the privacy rights of individuals and the surveillance powers of law enforcement authorities.

---

[64] TheBanks.eu website, "Compare Countries By Banking Sector", <https://thebanks.eu/compare-countries-by-banking-sector#ref_5> 10 June 2021.
[65] For the UK, FATF (2018) (n,44), 18. For Switzerland, FATF (2016) (n,43), 5
[66] For the UK, FATF (2018) (n,44), 5. For Switzerland, FATF (2016) (n,43), 5.
[67] For the UK, see FATF (2018), (n,44), 18. For Switzerland, see FATF (2016) (n,43), 3, 5 and (referring to Swiss National Risk Assessment report published in June 2015).
[68] People of Geneva were granted a unique privilege in Christendom by the Church in 1387: right to lend money at interest. Currently, Geneva is 9th largest financial centres in the world. M Hoffman, *Usury in Christendom: The Mortal Sin that Was and Now is Not* (Independent History and Research 2012), 83.
[69] A letter believed to have been written by Benjamin Franklin in 1755 on behalf of the Pennsylvania Assembly to the colonial governor.
[70] See B. Wittes, "What Ben Franklin Really Said", Lawfare Blog, 15 July 2011, <https://www.lawfareblog.com/what-ben-franklin-really-said> 10 June 2021.

The war against money laundering and underlying offences relies on information supplied by the financial industry filing their STRs.[71] The effectiveness of the STRs regime is subject to a vivid debate.[72] One problem of the STRs regime in most countries is the overwhelming number of unwarranted defensive reports. A significant issue leading reporters to make unwarranted disclosures is AML laws in breach of banking clients' right to privacy. This thesis defends this argument focusing on the SARs regime in two legal systems: England, which is famous with its strong AML laws,[73] and Switzerland, which is known for its strong financial secrecy laws.[74]

This thesis defends that re-designing the STRs regime in compliance with information privacy laws will increase the success in the fight against economic crime, criminal money and money laundering. Hence, it defends that those who fight for information privacy will also gain security.

This thesis contributes to the knowledge in three respects. First, this thesis provides an extensive explanation of the FATF recommendations and English and Swiss AML laws relating to banks' duty and right to make SARs. SARs regime related rules are complicated and misunderstood by many. Moreover, there is not enough resource written in English exploring relevant Swiss laws accurately. Furthermore, some provisions of relevant Swiss AML laws are mistranslated in the Federal Council's website. Hence, this thesis contributes to the knowledge by explaining this area of law in detail. Second, this thesis demonstrates that the main problem with AML laws relating to the SARs regime is the fact that lawmakers failed to take necessary measures against banks' misuse of relevant rules. While many authors argue that the main problem with relevant AML rules is the ambiguity of the suspicion term, this thesis shows that an informed group such as bankers can scarcely claim that they do not understand it. Third, this thesis shows that fighting against economic crime and protecting privacy are not contradicting aims by demonstrating the fact that SARs related AML laws in breach of privacy standards lead bankers to make unwarranted disclosures and unwarranted reports decrease law enforcement agencies' capacity to fight against economic crime, criminal money and money laundering.

Chapter 2. This thesis investigates AML laws relating to banks' duty and right to make SARs from the perspective of banking clients' right to the protection of personal data, and focuses on the recommendations adopted by the FATF and AML laws adopted by English and Swiss lawmakers. The SARs regime related AML rules are complicated, and most authors who work on criminal law, banking law or privacy laws related topics are not familiar with these rules. Therefore, the first chapter after introduction explores relevant FATF recommendations and English and Swiss AML laws, the rules that are to be investigated from the perspective of banking clients' right to the protection of personal data.

[71] P A Gallo and C C Juckes, 'Threshold transaction disclosures: access on demand through latent disclosure rather than reporting' (2005) 8(4) J.M.L.C. 328, 329.
[72] See footnote 7.
[73] FATF (2018) (n,45), 3.
[74] Tax Justice Network (n,53), 1.

While relevant rules are explored in chapter 2, the definition of economic crime and money laundering, the way in which and the reason why money launderers misuse banking services and products and the reason why bankers should be required to report their suspicions will be investigated in chapter 4 where the extent to which imposing upon banks a duty to make SARs is necessary for the detection, prevention and prosecution of crime is questioned.

Chapter 2 defends that modern AML laws made banks the private policemen of the financial sphere by imposing upon them three duties: (i) duty to report suspicious transactions, (ii) duty to undertake customer due diligence measures, and (iii) duty to apply a risk-based approach. Chapter 2 focuses on the first one of these duties. It explores the FATF recommendations and English and Swiss AML laws requiring and permitting banks to make STRs.

The FATF recommends countries to adopt laws requiring and permitting financial institutions to make STRs.[75]

English AML laws impose upon bankers duty to make two types of SARs: authorised reports or Defence against Money Laundering SARs and required SARs. Reporters are protected from criminal and civil liability for breach of any restriction on disclosure of information where they make an authorised or protected disclosure.

Swiss AML laws specified two types of SARs: reports specified in article 305*bis* of Swiss Criminal Code 1937 (ie. permitted SARs) and reports specified in article 9 (1) of Anti-Money Laundering Act 1997 (AMLA 1997) (required SARs). Banks are allowed to make an SAR where the conditions specified in article 305*bis* of Swiss Criminal Code 1937 are met. Moreover, banks are permitted and required to make an SAR where the conditions listed in article 9(1) of AMLA 1997 are met. Reporters in Switzerland are protected from criminal and civil liability for breach of any restriction on disclosure of information where they made a permitted or required disclosure in good faith.

Information privacy laws with which AML rules that were subjected to an extensive comparative analysis in chapter 2 should comply will be investigated in chapter 3.

Chapter 3. The FATF recommendations and English and Swiss laws recognised individual banking clients' *prima facie* exclusive control rights over their personal data. Therefore, the STRs regime should be compatible with information privacy laws. Chapter 3 investigates legal instruments in English and Swiss laws that protect banking clients' right to the protection of personal data.

The FATF remained silent about information privacy rights until 2018.[76] Currently, the FATF's recommendation 2 advises competent authorities to take necessary measures to guarantee compatibility

[75] Recommendations 20 and 21. FATF (n,4), 19.
[76] Privacy International (n,22).

of AML laws with data protection and privacy rules and other similar provisions.[77] The FATF officials did not further explain what data protection and privacy rules recommendation two is referring to.[78]

In English and Swiss laws, data protection acts protect banking clients' right to the protection of personal data. Some dispositions of the data protection acts apply to the banks' processing of personal data even where the processing of personal data is to comply with a legal duty to which the bank is subject. Moreover, the law of confidence has long but partially protected banking clients' control rights over their personal data. Furthermore, the European Convention of Human Rights, which has a special place in English and Swiss laws, protect banking clients' information privacy rights.

One argument defended in chapter 3 is that AML rules that interfere with banking clients' information privacy rights are justified if they are necessary for the detection, prevention and prosecution of economic crime. Chapter 4 investigates the extent to which imposing upon banks a duty to make SARs is necessary for the detection, prevention and prosecution of crime.

Chapter 4. This thesis defends that establishing a system where banks share their suspicions relating to the source origin of their client's funds with the Financial Intelligence Units (FIUs) is necessary to fight against money laundering and underlying offences. Chapter 4 is to show the place of the banking STRs in the fight against economic crime, criminal money and money laundering.

Countries have taken measures to fight against money laundering and underlying offences. First, lawmakers adopted confiscation measures to deprive economic criminals of the proceeds of crime. Second, 'laundering' proceeds of crime was criminalised to punish those who "conceal or disguise the identity of illegally obtained proceeds".[79] Law enforcement authorities can confiscate criminal money and punish money launderers and other economic criminals as far as they can detect illegal money and economic crime. Illegal money and economic crime are often caught by following suspicious money. Therefore, countries adopted measures to increase law enforcement agencies' capacity to detect suspicious money. One of these measures is establishing a system where banks are required and permitted to produce STRs. These reports may significantly help law enforcement authorities for two reasons. First, banks have the capacity to detect their client's suspicious activities accurately. Indeed, banks involve financial and legal experts who can distinguish their client's regular, unusual and suspicious financial activities and bankers have access to extremely useful financial information (eg. the client's financial transaction data). Second, regulating the banking industry is beneficial because economic criminals often misuse banking services and products to launder criminal proceeds.

[77] Recommendation 2. FATF (n,4), 10.
[78] FATF (n,4), 37, 87.
[79] "Money Laundering", Interpol web site, <https://www.interpol.int/Crime-areas/Financial-crime/Money-laundering> accessed 14 June 2018.

Therefore, banking STRs play a crucial rôle in the fight against money laundering and underlying offence. Gallo and Juckes explained the role of STRs in combating money laundering as follows:[80]

> It is popular to talk about *combating* money laundering and *war* against terrorist financing, but what must be appreciated in such a 'war' is that unlike conventional military conflicts against an opposing military force, a war against money laundering and terrorist financing cannot be fought by government forces alone; the entire intelligence gathering and target acquisition process is in the hands of the private sector. There are no reconnaissance troops scouting forward, no spy planes overhead, it is a war that relies on information supplied by the financial industry and others filing their STRs.

Chapter 5. This thesis defends that those who give up information privacy in order to gain security will not have either one. Chapter 5 shows that AML laws relating to the STRs regime, which are in breach of information privacy laws, lead bankers to make low-quality reports and low-quality reports shadow reports that may provide essential information. Goldby describes unwarranted reports as 'noise' which distract the attention of law enforcement agencies from the most serious or urgent cases.[81] This noise affects many countries, including the UK and Switzerland.

The FATF's recommendations 20 and 21 should be interpreted in compliance with data protection and confidentiality laws.[82] However, the FATF officials did not give sufficient weight to data protection laws in Interpretive notes to recommendations and Mutual Evaluation Reports.

This thesis defends that countries can fight against money laundering and underlying offences more successfully by adopting AML laws respecting individuals' right to the protection of personal data. Last part of chapter 5 makes recommendations to increase the effectiveness of the SARs regime by giving effect to information privacy laws. The FATF officials should take further steps to underline that the STRs regimes should be compatible with data protection and privacy standards. English and Swiss lawmakers should take sufficient and adequate measures to impede bankers abuse of the SARs regime.

[80] Gallo and Juckes (n,71), 329.
[81] M Goldby, 'Anti-money laundering reporting requirements imposed by English law: measuring effectiveness and gauging the need for reform' [2013] Journal of Business Law 367, 382.
[82] Recommendation 2, FATF (n,4), 10.

CHAPTER 2: THE SUSPICIOUS TRANSACTION REPORTS REGIME: THE FATF'S RECOMMENDATIONS, ENGLISH AND SWISS ANTI-MONEY LAUNDERING LAWS

2.I. Introduction

2.I.A. Arguments

This thesis investigates the Suspicious Transaction Reports (STRs) regime, focusing on the Financial Action Task Force's recommendations and English and Swiss Anti-Money Laundering (AML) laws. This chapter compares relevant Financial Action Task Force (FATF) standards and English and Swiss AML laws.

The FATF's recommendation 20 prescribes that a financial institution that suspects, or has reasonable grounds to suspect, that funds are the proceeds of criminal activity should be required, by law, to report promptly its suspicions to the financial intelligence unit.[1] The FATF, in its recommendation 21, advises countries to protect those who report their suspicions in good faith, from criminal and civil liability for breach of any restriction on disclosure of information.[2] The FATF also recommends countries to prohibit by law financial institutions and their staff from tipping-off. [3]

English AML laws specified two types of Suspicious Activity Reports (SARs): authorised reports and required reports. One who failed to make an appropriate authorised disclosure may be prosecuted with a principal money laundering offence.[4] One who failed to make a required disclosure "may be liable for prosecution for one of three disclosure offences, depending on their status and whether they were acting within or outside the regulated sector".[5] Authorised and required disclosures are "not to be taken to breach any restriction on the disclosure of information"[6]. Proceeds of Crime Act 2002 (POCA 2002) recognised tipping-off as a criminal offence.[7]

Swiss AML laws specified two types of SARs: permitted reports (Article 305*ter* paragraph 2 of Swiss Criminal Code 1937) and required reports (Articles 9 and 11 of Anti-Money Laundering Act 1997). Article 305*ter* paragraph 2 of the Swiss Criminal Code 1937 (SCC 1937) permitted financial institutions

[1] Recommendation 20. FATF (2012-2020), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, 19, <www.fatf-gafi.org/recommendations.html> 10 June 2021.
[2] Recommendation 21. FATF (n.1), 19.
[3] Recommendation 21. FATF (n.1), 19.
[4] Sections 327-329, POCA 2002
[5] Law Commission, Anti-money laundering: the SARs regime (Law Com No 236, 2018), [2.32].
[6] Sections 337-1 and 338-4, POCA 2002.
[7] Section 333A, POCA 2002.

to make SARs (permitted reports). Article 9(1) of the Anti-Money Laundering Act 1997 (AMLA 1997) imposes upon financial intermediaries a duty of making SARs (required reports). One who made a required disclosure in good faith is protected from criminal and civil liability for breach of any restriction on disclosure of information.[8] It is worth noting that permitted reports on the basis of Article 305*ter* paragraph 2 of SCC 1937 and required reports on the basis of Article 9(1) of AMLA 1997 are two different types of reports. Moreover, Swiss law-maker prohibited tipping-off.[9]

2.I.B. Key concepts: Suspicious transaction reports and other types of reports

There is a number of different types of reports banks are required to file with the law enforcement agencies, one of which is the STRs. This part explores the difference between the STRs and other reports (ie. suspicious activity reports (SARs) and threshold reports).

2.I.B.1. Suspicious Transaction Reports and Suspicious Activity Reports

Directors, officers or employees of a financial institution may suspect that their client's funds constitute or represent criminal money. SARs and STRs are reports by which the reporter discloses its suspicion to the designated law enforcement authority.

In an STR, the suspicion of the reporter is based on a transaction.[10] In an SAR, the reporting person shares its "suspicions raised around a customer's activity as a whole, not necessarily based on a transaction".[11] Hence, the STRs is a subset of the SARs.

The FATF recommends countries to establish a mandatory STRs regime that applies to financial institutions.[12] English and Swiss AML laws went further, imposing upon financial institutions duty to make SARs.[13]

[8] Article 11(1), AMLA 1997.
[9] Article 10a, AMLA 1997; and article 47, Swiss Banking Act 1934.
[10] Europol Report, 'From suspicion to action: Converting financial intelligence into greater operational impact' (2017), 41 <https://www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact> 1 June 2021.
[11] Ibid.
[12] Recommendations 20 and 21. FATF (n.1), 19.
[13] See sections 327-331 and 338, POCA 2002; and article 9(1), AMLA 1997.

2.I.B.2.b. Threshold reports

Some legal systems imposed upon financial institutions duty to make reports based on objective indicators.[14] These reports (eg. cash placement reports that bankers are required to make when a client place money into the financial system above a threshold, financial transaction reports that bankers are required to produce upon a financial transaction above a threshold, and international financial transaction reports that bankers are obliged to make upon an international financial transaction above a threshold) are named as threshold reports.[15]

In its recommendations 2003, the FATF advised countries to consider "the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount".[16] The FATF abolished this recommendation in 2012. Most EU countries do not impose upon banks duty to produce threshold reports.[17]

Another type of report is the Unusual transaction reports (UTRs). Dutch law imposes upon financial institutions duty to make a UTR if at least one of the objective indicators (eg. a transaction for a sum of €10,000 or more that involves the exchanging of cash into other currencies or from small to large denominations of banknotes, a cash deposit for a sum of €10,000 or more in favour of a credit card or a prepaid instrument of payment, or the use of a credit card or a prepaid instrument of payment in connection with a transaction for the sum of €15,000 or more) or the subjective indicator (ie. relevant person has reason to believe that a transaction might be related to money laundering or terrorism financing) is met.[18] Hence, UTRs cover both STRs and threshold reports. Therefore, the number of reports received by the Netherland's FIU is very high. In its 2017 report, Europol established that the Netherlands' FIU received the second-highest number of reports in the EU between 2006 and 2014.[19]

[14] The USA, Canada and Australia are amongst the countries which require financial institutions to produce threshold reports. See B Unger and F V Waarden, 'How to Dodge Drowning in Data: Rule- and Risk-Based Anti Money Laundering Policies Compared" (2009) 5 Rev. L & Econ. 953, 957-959.

[15] A Joshi, 'In Pursuit of Big Data: An Analysis of International Funds Transfer Reporting' RUSI Occasional Paper, April 2017, 17 <https://rusi.org/sites/default/files/201704_rusi_in_pursuit_of_big_data_joshi.pdf> 10 June 2021.

[16] Recommendation 19. FATF, The Forty Recommendations, 20 June 2003, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf> 10 June 2021.

[17] Europol (n.10), 41.

[18] Section 16, Money Laundering and Terrorist Financing (Prevention) Act (Wwft).

[19] According to the Europol's report published in 2017, 67% of the SARs in the EU were received by the FIUs in two member states: the UK (36%) and Netherlands (31%). See Europol (n.10), 10, chart 2. According to chart 2, the UK FIU and the Netherlands' FIU received 67% of total reports across all Member States (2006 - 2014). Yet, this was mistakenly mentioned as 65% of total reports in pages 5 and 10 of the report.

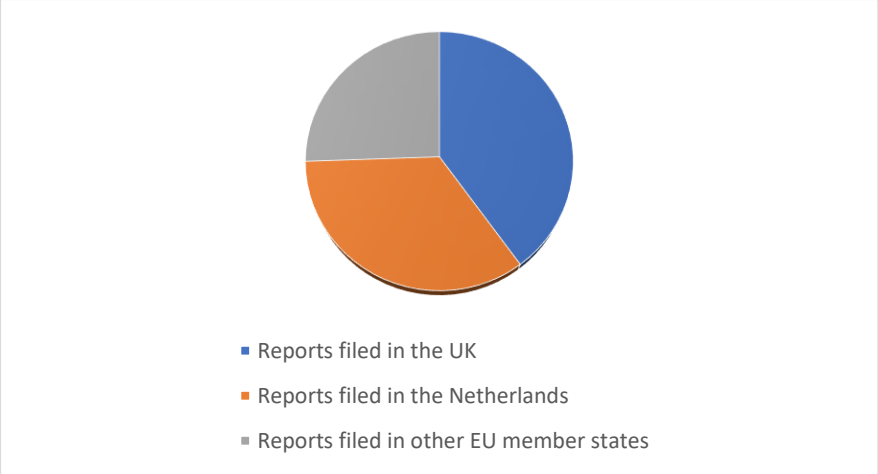


Chart 3: Number of reports the private sector made from 2006 to 2014.

2.II. Bankers as the private policemen of the financial sphere

2.II.A. Introduction

Economic criminals have long misused banking products and services to launder the proceeds of crime. To protect banks from the threat of money laundering, lawmakers provided banks and their staff with some policeman duties and privileges. First, banks are permitted and required to report their suspicions concerning the source origin of their client's assets. Second, banks are permitted and required to know their clients. Moreover, they are "expected to identify, assess and understand the money laundering … risks to which they are exposed and take AML.. measures commensurate to those risks in order to mitigate them effectively"[20].

2.II.B. Historical overview

2.II.B.1. From hands-off approach to private policeman duties and privileges

2.II.B.1.a. Early 20th century

Most legal systems had recognised banks' legal duty of secrecy by the end of the 1920s.[21] Banks' legal duty of confidentiality was not unimpeachable. For instance, banks were required to share confidential information with competent public authorities where it is necessary for the prevention and prosecution of crime. However, bankers were not seen as the private policemen of the financial sphere. Neither they

[20] FATF, 'Guidance for A Risk-based approach - the banking sector' October 2014, 6 <http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf> 10 June 2021.
[21] See pages 101-104 in following chapter 3.

were under a duty to report their client's suspicious activities with law enforcement authorities, nor were they obliged to interlope with their client's financial affairs to detect criminal money. In most legal systems, the bank-client relations were regulated with a hands-off approach.[22] Bankers were obliged to engage with their customers' finances only if and the extent to which they owed a duty to act with a standard of care and skill when dealing with the clients. Bankers' duty of care may be subjected to an extensive examination.[23] However, what is essential for this chapter is that bankers' duty of care did not extend to policeman duties (ie. Know your customer and suspicious activity reporting duties). Sankey LJ put it in 1929 that bankers were not required to subject their customer's account to a 'microscopic examination', and banking officials were not expected to be 'amateur detectives'[24]. In Switzerland, the hands-off approach was even more potent. Banks were allowed to open numbered accounts where the customer's identity was replaced by a multi-digit number or a code name.[25]

2.II.B.1.b. From the 1960s onward

In the second half of the 20th century, many countries declared a fight against criminal money.[26] Economic criminals had long been misusing banking products and services to cleanse illicit money. To increase the success in fighting against economic crime and criminal money, legislators decided to establish strong cooperation between law enforcement authorities, on the one hand, and financial institutions, including banks, on the other hand.[27] Swiss and English lawmakers played an essential role in this process. The Swiss Bankers Association formed the basis of customer due diligence regulations with the Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence

[22] J Thomas, 'Money laundering in the 21st century: Follow the money' Payments Cards & Mobile website <http://www.paymentscardsandmobile.com/money-laundering-in-the-21st-century/> 9 June 2021.

[23] English and Swiss courts applied several different tests to establish whether or not a banking institution may be accepted as having acted in negligence. Sankey LJ in *Llyods Bank v The Chartered Bank of India, Australia and China* [1929] 1 KB 40, 73 had given following examples: "[A] bank may be negligent in not making inquiries as to a customer on opening an account: Ladbroke & Co. v. Todd (1); Commissioners of Taxation v. English, Scottish and Australian Bank (2); and there may be negligence in not noticing the account of the customer from time to time and considering whether it is a proper or a suspicious one : Morison's case. (3)".It is worth mentioning that these cases cited by Sankey LJ are cases in which a stolen cheque (*Ladbroke and Co v Todd* (1914) 30 TLR 433 and *Commissioners of Taxation v English, Scottish and Australian Bank Limited* (1920) AC 683) or a cheque signed per pro in fraud of the authority (*Morison v London County and Westminster Bank, Limited* [1914] 3 K. B. 366) had been cleared by a bank without sufficient examination. Similarly, according to the Swiss Federal Supreme Court's jurisprudence, bankers were required to investigate their clients' account in order to comply with their duty of care and fidelity. See C Lombardini, *Droit bancaire Suisse* (2eme ed, Schulthess 2008), 68-75.

[24] *Llyods Bank v The Chartered Bank of India, Australia and China* [1929] 1 KB 40, 73 (by Sankey LJ)

[25] See Article 4 of the Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence 1977; and Lombardini (n.23), 93.

[26] The 1988 UN Vienna Convention, the first UN Convention that requires criminalisation of laundering drug money, of money and the Palermo Convention 2000 and the Protocols thereto, which extended the scope laundering offence, have 191 and 190 state parties respectively.

[27] J Wadsley, 'Money laundering: professionals as policemen' (1994) Conv. 275, 277.

1977 (CDB 1977).[28] English law-maker laid the foundation of SARs rules with section 24 of Drug Trafficking Offences Act 1986.[29]

The FATF was established in 1989 to examine and develop measures to combat money laundering.[30] In 1990, the FATF issued its forty recommendations on money laundering, which advised countries to create an AML system where law enforcement authorities and financial institutions (ie. banks and non-bank financial institutions) cooperate in fighting against criminal money.[31] Within the context of this cooperation, the FATF recommended countries to give financial institutions the duty or right to report their client's suspicious transactions with competent public authorities.[32] Duty or right to report in the recommendations 1990 became duty and right to report in the recommendations 2003.[33] To enhance banks' capacity to detect their client's suspicious transactions, the FATF recommended countries to require financial institutions to undertake customer due diligence (CDD) and record-keeping measures.[34] Hence, countries were advised to replace the traditional hands-off approach with the principle of Know Your Customer. [35] Thus, the FATF advised countries to make banks and non-bank financial institutions the private policemen of the financial sphere.

2.II.B.2. From rule-based and case-based approaches to a risk-based-approach

AML laws adopted in the late 20th century granted banks restricted discretionary powers. In the wake of the 21st century, lawmakers broadened banks' discretionary power by accepting a risk-based approach.[36] With the adoption of the risk-based approach, banks were upgraded from police officers who execute orders to police chiefs involved in the evolution of policies.

---

[28] See Convention relative à l'obligation de diligence des banque 1977 of the Swiss Bankers' Association.

[29] According to Section 24 of Drug Trafficking Offences Act 1986, one who assists another to retain the benefit of drug trafficking knowing or suspecting that the other person carries on or has carried on drug trafficking or has benefited from drug trafficking is guilty of an offence. However, one does not commit such crime if he discloses properly to a constable a suspicion or belief that any funds or investments are derived from or used in connection with drug trafficking or any matter on which such a suspicion or belief. For a further investigation, see B Unger, 'Money Laundering Regulation: from Al Capone to Al Qaeda' in B Unger and D vaan der Linde (eds), *Research Handbook on Money Laundering* (Edward Elgar 2013), 23.

[30] 'Economic Declaration', Paris, 16 July 1989. <http://www.g8.utoronto.ca/summit/1989paris/communique/index.html> 10 June 2021.

[31] Recommendation 9, FATF, The Forty Recommendations of the Financial Action Task Force on Money Laundering 1990, <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf> 10 June 2021.

[32] Recommendation 16, Ibid.

[33] Recommendations 13 and 14, FATF (n.16).

[34] Recommendations 12-20, FATF (n.31); and Recommendations 5-11, FATF (n.16).

[35] Thomas (n.22).

[36] In relation to the acceptance of a RBA in the recommendations 2003 and 2012, see Recommendation 15, FATF (n.16); and Recommendation 1, FATF (n.1), 10.

The risk-based approach (RBA), which now constitutes one of the central elements of the contemporary AML laws, entered into the FATF's recommendations in 2003. Previously, rule-based and case-based approaches were preferred.

The FATF recommendations 1990 established a rule-based AML system.[37] In a rule-based system, prescriptive rules oblige relevant persons to do or not to do certain activities. A frequently used example for a rule-based system is traffic rules. If exceeding the specified speed limit is prohibited, it is prohibited in all contexts and all cases. Rule-based systems should be preferred to regulate matters that are not context or case-sensitive.[38] Money-laundering, however, "operates through the use of financial activities which are not in themselves illegal. An activity that in one context is money laundering may in another context be entirely legal"[39]. Therefore, the rule-based system was supported with a case-based system. In a case based approach, relevant persons should work for describing "the key characteristics of distinctive forms of money laundering … so that other parties can detect this kind of activity". [40] Case studies and typology reports are frequently used in a case-based system.[41]

Risk-based approach (RBA) works through the evaluation of some simple risk factors rather than idealized type cases. Ross and Hannan explained the risk-based approach as follows: [42]

> Unlike case-based decision-making, where in effect we are asking "does this combination of client and transaction attributes match a known pattern associated with money laundering?", a risk based approach requires that we have a probabilistic model that shows how specific attributes of the problem space contribute to the probability that money laundering is present.[43]

According to the FATF's recommendation 1, financial institutions should be required to apply a RBA.[44] A RBA to AML for banks means that they "are expected to identify, assess and understand the money laundering … risks to which they are exposed and take AML … measures commensurate to those risks in order to mitigate them effectively"[45]. The general principle of a RBA is that, "where there are higher risks, relevant persons should take enhanced measures to manage and mitigate those risks; and that,

[37] S Ross and M Hannan, 'Money laundering regulation and risk- based decision making, (2007) 10(1) J.M.L.C. 106, 108. Threshold reports regime, where financial institutions are required to report transactions above a threshold, reflect a rule-based approach.
[38] Ibid, 109
[39] Ibid.
[40] Ibid.
[41] Ibid.
[42] Ibid, 110.
[43] Ibid.
[44] Recommendation 1, FATF (n.1), 10. Chapter 2 of the UK Money Laundering Regulations 2017 is dedicated to specify rules relating to the application of a RBA by supervisory authorities and relevant persons such as banks. Swiss AMLA 1997 does not have a particular section to specify RBA-related rules, but explains it separately in diverse sections relating to particular AML rules. Further details are determined in relevant industry guidance(s) in both the UK and Switzerland.
[45] FATF (n.20), 6.

correspondingly, where the risks are lower, simplified measures may be permitted".[46] Accordingly, banks are required to identify and assess their money laundering risks for customers (eg. regrouping customers as high, medium and low-risk customer profiles), countries or geographic areas; and products, services, transactions or delivery channels.[47] This risk assessment should provide the basis for the risk-sensitive application of AML measures.[48]

Banks that are required to undertake AML measures in a risk-sensitive manner are profit-oriented entities. Lawmakers took measures against banks' misuse of the RBA. First, banks can undertake simplified measures if relevant AML rules permitted them to do so.[49] Second, banking supervisors[50] "assess whether a bank's policies, procedures and controls are appropriate in view of the risks identified through the risk assessment, and its risk appetite".[51]

2.II.C Bankers' duty of reporting

Directors, officers or employees of a banking institution may suspect that their client's funds constitute or represent criminal money. The banking staff's assessment concerning its client's financial affairs is highly likely to be accurate due to two reasons. First, banking staff have access to a wide range of information relating to their clients, enabling them to know their clients (eg. financial transaction data, customer due diligence information).[52] Second, banking staff involve financial and legal experts who can successfully distinguish their client's expected, unusual and suspicious activities.[53]

Bankers should take the transactions that they find suspicious seriously. First, when they suspect that their client's assets constitute or represent criminal money, they need to undertake additional CDD measures to understand who their customer is, what does he/she do and why does he/she require banking

[46] Interpretive Note to Recommendation 1, FATF (n.1), 31.
[47] Ibid.
[48] FATF (n.20), 6.
[49] FATF (n.20), 15.
[50] Banks are dual-regulated in the UK, by both the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA). The former is the primary regulator so far as regulation in relation to financial crime is concerned. (R Brent, 'Regulatory Responsibilities' in W Blair, R Brent and T Grant (eds) *Banks and financial crime – the international law of tainted money* (2nd edn, OUP 2017), 249.) Banks in Switzerland are regulated by the Swiss Financial Market Supervisory Authority (FINMA), which replaced three supervisory authorities in 2009. FINMA's predecessors are the Anti-Money Laundering Control Authority (AMLCO), the Swiss Federal Banking Commission (SFBC) and the Federal Office of Private Insurance (FOPI). Both British and Swiss financial supervisors, the FCA and the FINMA, are independent authorities.
[51] FATF (n.20), 15.
[52] See R Parlour, 'Practicalities of Financial Crime Deterrence' in B Rider (ed), *Research Handbook on International Financial Crime* (Edward Elgar Publishing 2015), 305; and A Bacarese, K Levy and H Mulukutla, 'The management of information in the context of suspected money laundering cases' in B Rider (ed), *Research Handbook on International Financial Crime* (Edward Elgar Publishing 2015), 513; and Thomas (n.22).
[53] For further details, see chapter 4.

services.[54] A banker who takes no further action to eliminate its suspicion takes the risk of disregarding or even facilitating criminal activity.

Bankers are private persons, and they do not have investigative powers. They cannot always find adequate and sufficient information by undertaking CDD measures to set aside their suspicion. A banker who could not set aside his suspicion should share its suspicion with competent public authorities. The public authority with whom the banks can share their suspicions should use information disclosed by the banks in two ways[55]. First, they should use the STRs "to identify specific targets (e.g. persons, assets, criminal networks and associations)".[56] Second, they should use the STRs "to identify money laundering and terrorist financing related trends and patterns". [57]

Initially, the STRs regime was applied to 'banks and non-bank financial institutions' only.[58] Currently, the STRs regime extends to designated non-financial businesses and professions (eg. lawyers, casinos) subject to certain qualifications.[59]

2.II.D. Banking institutions' Know Your Customer duties

2.II.D.1. Introduction

Bankers can accurately distinguish their client's expected, unusual and suspicious activities if they have accurate and adequate information relating to their customers and analyse such information adequately. Customer Due Diligence (CDD) and record keeping rules are to guarantee the accuracy and adequacy of banking data and its adequate examination by banks. Thus, these rules aim to increase banks' capacity to detect their clients' unusual or suspicious activities accurately.

Banks are required to know their customers by undertaking CDD and record-keeping measures.[60] The FATF Recommendations 10 to 19 laid down banks' CDD and record-keeping duties. English and Swiss law-makers took measures to comply with these recommendations.[61]

---

[54] Recommendation 10(2), FATF (n.1), 19; and FATF (n.20), 19.; (UK) Anti-Money Laundering Regulations 2017, Article 27(2)(c); (CH) Article 6(2) of AMLA 1997.
[55] Interpretive note to recommendation 29, FATF (n.1), 101-103.
[56] Ibid.
[57] Ibid.
[58] Recommendations 9 and 16. 'The Forty Recommendations of the Financial Action Task Force on Money Laundering 1990' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf> 10 June 2021.
[59] Recommendations 12 and 16, FATF (n.16); and Recommendations 20 and 23 FATF (n.1), 19-20.
[60] Recommendations 10 and 11, FATF (n.1), 14-15.
[61] English law relating to banks' CDD duties may be found in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (Regulations 2017), the Financial Services and Markets Act 2000 (FSMA 2000), the Financial Conduct Authority Handbook (FCA Handbook), the Financial

2.II.D.2. Customer Due Diligence measures

FATF recommends countries to prohibit anonymous accounts or accounts in obviously fictitious names.[62] Banks are required to know their clients by undertaking CDD measures.

> Where the financial institution is unable to comply with the applicable [CDD] requirements…, it should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.[63]

Prohibition of anonymous accounts has been a radical step for countries famous for their secrecy laws, such as Switzerland, where the bearer savings books system was an essential institution until the 1960s.[64]

KYC rules determine when banks ought to undertake customer due diligence measures and what information they ought to have relating to their clients.

2.II.D.2.a. When are banks required to apply CDD measures?

Banks are required to undertake CDD measures before establishing business relations (initial due diligence).[65] The FATF's guidance for the banking sector established that [66]

Conduct Authority Guidance (FCA Guidance). The main legal instrument where banks' CDD and record-keeping duties are determined is Regulations 2017. Moreover, under Part 9A of the FSMA 2000, the Financial Conduct Authority (FCA), which regulates the banking industry in relation to financial crime, is empowered to make rules applying to banks and other financial institutions. The FCA's relevant rules are contained in 'the FCA Handbook'. The rules relating to the prevention of financial crime may be found in 'the Principles for Business' (PRIN) and 'the Senior Management Arrangements, Systems and Controls' (SYSC) sections of the Handbook. The FCA produced a guidance, where relatively brief rules in the Handbook are explained. Besides, another guidance for the UK financial sector was issued by the Joint Money Laundering Steering Group (JMLSG). While the FCA Guidance and the Joint Money Laundering Steering Group Guidance (JMLSG Guidance) are not binding, they have statutory backing[61]. The former is adopted in accordance with section 157 of FSMA 2000, while the latter has statutory support in the SYSC 6.3.5 of the FCA Handbook. For further information, see Brent (n.50), 251.
Swiss AML laws relating to banks' due diligence duties may be found in four legal instruments. First, Article 305*ter* of the SCC 1937 set forth jail terms for failing to conduct some specified due diligence measures. Second, the Anti- Money Laundering Act 1997 (AMLA 1997) lays down basic rules relating to relevant persons' due diligence duties. Third, 'the FINMA Anti-money laundering ordinance' (OBA-FINMA) explained these basic rules. According to Article 12 of AMLA 1997, financial intermediaries, including banks, may be supervised by the recognised self-regulatory organisations, or FINMA, where the financial intermediaries are not affiliated to a recognised self-regulatory organisation. The recognised self-regulatory organisation for the banking sector in accordance with Article 24 of AMLA is the Swiss Bankers' Association. 'Swiss Bankers Association's Code of Conduct with regard to the exercise of due diligence' specify due diligence duties of the financial intermediaries. To conclude, Swiss law relating to banks' due diligence duties may be found in SCC 1937, AMLA 1997, OBA-FINMA and Swiss Bankers Association's Code of Conduct with regard to the exercise of due diligence.

[62] Recommendation 10, FATF (n.1), 14-15.

[63] Ibid.

[64] See Article 4 of the Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence 1977; and Lombardini (n.23), 93.

[65] The FATF Recommendations, *Recommendation 10(2)*; (UK) Anti-Money Laundering Regulations 2017, *Article 27(2)(a)*; and (CH) AMLA 1997, *Articles 3(1) and 6(1)*.

[66] FATF (n.20), 19.

> The initial stages of the CDD process should be designed to help banks assess the ML/TF risk associated with a proposed business relationship, determine the level of CDD to be applied and deter persons from establishing a business relationship to conduct illicit activity.

Moreover, banks must undertake CDD measures during their professional relationship with their clients (ie. ongoing due diligence). First, banks are required to undertake CDD measures carrying out occasional transactions above a designated threshold.[67] Second, they are required to undertake CDD measures when there is a suspicion of money laundering or terrorist financing.[68] Third, they are required to undertake CDD measures when they have doubts about the veracity or adequacy of previously obtained customer identification data.[69] In addition, banks are required to apply CDD measures at other appropriate times to existing customers in a risk-sensitive manner.[70]

2.II.D.2.b. What is the content of the CDD measures?

The FATF's guidance for the banking sector established that "customer due diligence processes should be designed to help banks understand who their customers are by requiring them to gather information on what they do and why they require banking services."[71] Banks should produce their clients' customer, business and risk profiles in order to determine their true identity and "the type of activity that is expected, usual and normal for them"[72].

Banks are required to take measures against offenders who wish to launder criminal money by hiding their identity. To understand who their customers are, banks should identify "the customer and verify the customer's identity using reliable, independent source documents, data or information".[73] Banks should also identify "the beneficial owner, and take reasonable measures to verify the identity of the

[67] The FATF Recommendations, *Recommendation 10(2)*; (UK) Anti-Money Laundering Regulations 2017, Article 27 (2); and (CH) OBA-FINMA *Art. 40, 41, 51 and 61*.
[68] The FATF Recommendations, *Recommendation 10(2)*; (UK) Anti-Money Laundering Regulations 2017, *Article 27(2)(c)*; (CH) AMLA 1997 *Article 6(2)*.
[69] Recommendation 10(2), The FATF Recommendations; (UK) Anti-Money Laundering Regulations 2017, Article 27(2)(d); (CH) Article 5 of AMLA 1997
[70] Recommendation 10(8), The FATF Recommendations; (UK) Anti-Money Laundering Regulations 2017, Article 27 (8)-(9); (CH) Article 6(2) of AMLA 1997.
[71] FATF (n.20), 19.
[72] Thomas (n.22).
[73] Recommendation 10(4), The FATF Recommendations; (UK) Anti-Money Laundering Regulations 2017, Section 28 (1), (10) and (18); (CH) AMLA 1997, Article 3.

beneficial owner."[74] Furthermore, banks should understand the ownership and control structure of their customers where the customer is a legal person or arrangement.[75]

Banks are required to understand the purpose and intended nature of the business relationship with the client.[76] They are also required to conduct

> scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.[77]

In case of inconsistency, they should report promptly their suspicions to the FIU.[78]

Banks should undertake CDD measures in a risk-sensitive manner.[79] While some customers[80], businesses[81], and transaction services[82] require enhanced CDD measures, simplified CDD measures may suffice for some other customers[83], businesses[84] and transactions. Content of simplified or enhanced CDD measures should be determined with a RBA. The FATF's Interpretive note to recommendation 10 and the FATF Risk-based approach guidance for the banking sector listed some examples of enhanced and simplified due diligence measures.[85]

According to the FATF's Recommendation 12, banks should apply further CDD measures when their client or prospective client is a foreign politically exposed person (PEP), or a family member or a close

[74] Recommendation 10(4), The FATF Recommendations; (UK) Anti-Money Laundering Regulations 2017, Section 28 (4); (CH) article 4 of the AMLA 1997
[75] Recommendation 10(4), The FATF Recommendations; (UK) Anti-Money Laundering Regulations 2017, Section 28 (3),(4); (CH) AMLA 1997, Article 3.
[76] Recommendation 10(4), The FATF Recommendations; (UK) Anti-Money Laundering Regulations 2017, Section 28 (2); (CH) article 6(1) of the AMLA 1997
[77] FATF Recommendation 10, *Customer due diligence ; (UK)* Anti-Money Laundering Regulations 2017, Section 28 (11).
[78] Recommendation 10, FATF (n.1), 14-15.
[79] Interpretive note to recommendation 10, FATF (n.1), 67. For further details see. FATF (n.20), 20, box 3 ; for the UK, see Anti-Money Laundering Regulations 2017, Section 28(12) and 18(1); for Switzerland, see Articles 4 and 6 of AMLA 1997.
[80] Eg. non-resident customers, legal persons or arrangements that are personal asset-holding vehicles. See FATF (n.1), 66-70.
[81] Eg. private banking, non-face-to-face business relations and business that are cash-intensive. FATF (n.1), 66-70.
[82] Eg. anonymous transactions, all unusual patterns of transactions that have no apparent economic or lawful purpose and payment received from unknown or un-associated third parties. FATF (n.1), 66-70.
[83] Eg. public companies listed on a stock exchange and subject to disclosure requirements. FATF (n.1), 66-70.
[84] Eg. life insurance policies where the premium is low. FATF (n.1), 66-70.
[85] Examples of simplified due diligence measures: obtaining less information, seeking less robust verification, of the customer's identity and the purpose and intended nature of the business relationship, postponing the verification of the customer's identity (FATF (n.20), 20, box 3).
Examples of enhanced due diligence measures: Obtaining additional information on the source of funds or source of wealth of the customer or on the reasons for intended or performed transactions, commissioning an intelligence report on the customer to understand better the risk that the customer may be involved in criminal activity. (FATF (n.1), 66-70; FATF (n.20), 6.20, box 3)

associate of a PEP.[86] In addition, banks should apply further measures when they work with cross-border correspondent banking institutions.[87]

2.II.D.3. Record keeping duties.

The FATF advises countries to require financial institutions to maintain, for at least five years, all necessary records on transactions and all records obtained through CDD measures.[88] "The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority."[89]

English and Swiss AML laws relating to bankers duty of record-keeping are assessed compliant with the requirements of the FATF's recommendation 11.[90] English law requires banks to retain relevant records for a minimum of five years after the termination of the business relationship or after completion of the transaction.[91] Swiss law requires banks to retain the records for a minimum of ten years after the termination of the business relationship or after completion of the transaction.[92]

2.II.E. Conclusion

Economic criminals have long misused banking products and services to launder the proceeds of crime.[93] To protect banks from the threat of money laundering, lawmakers provided banks and their

[86] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 is significantly different than the Money Laundering Regulations 2007 (the Regulations 2007) as far as the PEP rules are concerned. This difference stems from the 5th EU Money Laundering Directive. The Regulations 2007, in accordance with the third EU Money laundering directive, defined a PEP as an individual who have been entrusted with prominent public functions (eg. members of parliament, the senior judiciary etc.) by a state other than the UK, by a Community institution, or by an international body. Hence, the UK PEPs were excluded. According to the Recital 25 of the third EU Money Laundering Directive, the "individuals holding or having held important public positions" banks were most at risk were "particularly those from countries where corruption is widespread" The Fifth EU Money Laundering Directive and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 accepted a wider PEP definition, which includes both national and foreign PEPs (The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, regulation 35(14)).
Definition of PEP in article 2a of AMLA 1997 covers both domestic and foreign politically exposed persons as well as their family members and close associates. However, there are different rules that apply in relation to foreign and domestic PEPs. (Article 6(3) and 6(4) of AMLA 1997)

[87] Recommendation 13, FATF (n.1), 17.

[88] Recommendation 11, FATF (n.1), 15.

[89] Ibid.

[90] FATF (2018), Anti-money laundering and counter-terrorist financing measures – United Kingdom, Fourth Round Mutual Evaluation Report, FATF, Paris available at: http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-kingdom2018.html at 161;
FATF (2016), Anti-money laundering and counter-terrorist financing measures - Switzerland, Fourth Round Mutual Evaluation Report, FATF, Paris, available at: www.fatf-gafi.org/publications/mutualevaluations/documents/mer-switzerland-2016.html at 183.

[91] Anti-Money Laundering Regulations 2017, Regulation 40.

[92] AMLA 1997, Article 7.

[93] The reason why and the way in which criminals misuse banking products and services will be further explored in chapter 4.

staff with some policeman duties and privileges. As the private policeman of the financial sphere, banks are required and permitted to make an SAR where they suspect, or have reasonable grounds to suspect, that their client's funds constitute or represent proceeds of crime. AML laws adopted in the 21st century broadened banks' discretionary power. With the adoption of a risk-based approach, banks were upgraded from police officers who execute orders to police chiefs involved in the evolution of policies.

2.III. The FATF recommendations

2.III.A. Introduction

The FATF advises countries to establish a system where financial institutions share their money-laundering suspicions with the Financial Intelligence Units (FIUs).

2.III.B. Evolution of the FATF's STRs regime related recommendations

The FATF, that was established in 1989 to develop measures to combat money laundering, released its forty recommendations in 1990.[94] The FATF advised countries to take measures increasing law enforcement agencies' capacity to detect criminal money and economic crime.[95] In its' recommendation 16, the FATF recommended countries to establish voluntary or mandatory STRs regime that applies to financial institutions (ie. banks and non-bank financial institutions) [96]. The first sentence of the relevant recommendation was as follows: "If financial institutions suspect that funds stem from a criminal activity, they should be permitted or required to report promptly their suspicions to the competent authorities." [97]

Establishing a system where financial institutions report their suspicions on their own initiative was a surprising and challenging objective in the 1990s.[98] Even some 12 years after the FATF's recommendations released in 1990, Mr Boris Johnson MP was perplexed in face of the idea of giving private entities a duty of suspicious activity reporting. He expressed his mix with the following questions:[99]

[94] "Economic Declaration" (n,30).
[95] Eg. Recommendations 14, 15, 16, 21, 24, 30 and 32. FATF (n.31).
[96] See Recommendations 9 and 16, FATF (n.31).
[97] See Recommendation 16, FATF (n.31).
[98] Wadsley (n.27), 276.
[99] Mr Boris Johnson MP, 2002. via R Stokes, 'The Banker's Duty of Confidentiality' (PhD thesis, University of Liverpool 2005), 57.

> How can an accountant *[for example]* have a professional relationship with his client if he goes around sneaking ... [H]ow can that relationship be possible if the accountant is sneaking to all and sundry about his private transactions with his clients?

Financial institutions are profit-oriented entities, and they risk their attractiveness by making STRs. Indeed, a bank may lose its financial attractiveness where the people learn that it is sneaking about its client's private transactions and informing public authorities of some of these transactions. Therefore, voluntary STRs regimes were unsuccessful in persuading banks to report their suspicions with competent public authorities.[100] Switzerland's 1994-1997 experience constitutes an important example that shows the failure of voluntary reporting systems.[101]

In 2003, the FATF amended its' STRs regime related recommendations and advised countries to establish a mandatory reporting system.[102] Recommendation 13 advised countries to require financial institutions, directly by law or regulation, to report their suspicions where they suspect or, have reasonable grounds to suspect that funds are the proceeds of criminal activity or are related to terrorist financing. Recommendation 14 underlined that countries should protect reporting persons from criminal and civil liability for breach of any restriction on disclosure of information if they report their suspicions in good faith. Current FATF recommendations, updated October 2020, follow the structure adopted in 2003.[103]

Recommendations released in 1990 did not make advice relating to the way in which the competent public authorities should use the STRs. Currently, the FATF recommends countries to

> establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis.[104]

The FIUs should benefit from the STRs in two ways. First, the FIUs should us the STRs

> "to identify specific targets (e.g. persons, assets, criminal networks and associations), to follow the trail of particular activities or transactions, and to determine links between those targets and possible proceeds of crime, money laundering, predicate offences or terrorist financing".[105]

Second, they should use the STRs to identify money laundering related trends and patterns. [106]

[100] Interpretive note to recommendation 20, FATF (n.1), 87.
[101] See pages 65-66.
[102] See Recommendations 13 and 14, FATF (n.16).
[103] Recommendations 20 and 21, FATF (n.1), 19.
[104] Recommendation 29, FATF (n.1), 24.
[105] Interpretive note to recommendation 29, FATF (n.1), 101.
[106] Ibid.

2.III.C. Financial institutions' duty of reporting and the FATF's recommendation 20

The FATF's recommendation 20 reads as follows: "If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit."

The FATF advises countries to impose upon 'financial institutions' a duty of reporting. The FATF's general glossary defines "financial institution" with reference to a long list of financial activities or operations.[107] "Any natural or legal person who conducts as a business one or more of the [listed] activities or operations for or on behalf of a customer" is considered as a financial institution.[108] Therefore, all types of banks are accepted as financial institutions.[109] It is worth noting that Recommendation 23 extended the duty of reporting to designated non-financial businesses and professions (eg. lawyers and casinos) subject to certain qualifications.

The subtitle of recommendation 20 is "Reporting of suspicious transactions". According to the FATF's relevant recommendation, countries should require financial institutions to report 'transactions' where they suspect or have "reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing".[110] Interpretive note to recommendation stressed that "[a]ll suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction".[111] Hence, recommendation 20 advises countries to establish a mandatory STRs regime.

"Criminal activity" in recommendation 20 refers to "all criminal acts that would constitute a predicate offence for money laundering or, at a minimum, to those offences that would constitute a predicate offence, as required by Recommendation 3."[112] The FATF recommends countries to adopt the first of these alternatives.[113]

According to the FATF's recommendation 3, "[c]ountries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences." Countries may describe predicate offences in a number of different ways: by reference to all offences, applying a

[107] 'Financial institutions', General Glossary, FATF (n.1), 119, 120.
[108] Ibid.
[109] Ibid.
[110] Recommendation 20, FATF (n.1), 19.
[111] Interpretive Note to Recommendation 20, FATF (n.1), 87.
[112] Ibid.
[113] Ibid.

threshold approach, by reference to a list of predicate offences or a combination of these approaches.[114] The interpretive note to recommendation provides that:[115]

> Where countries apply a threshold approach, predicate offences should, at a minimum, comprise all offences that fall within the category of serious offences under their national law, or should include offences that are punishable by a maximum penalty of more than one year's imprisonment, or, for those countries that have a minimum threshold for offences in their legal system, predicate offences should comprise all offences that are punished by a minimum penalty of more than six months imprisonment.

Money laundering is a universal challenge.[116] Therefore, the FATF provides that[117]

> Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically. Countries may provide that the only prerequisite is that the conduct would have constituted a predicate offence, had it occurred domestically.

The FATF is an intergovernmental authority that adopted a risk-based approach, which defends that[118]

> Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified.

Therefore, the organisation adopted general recommendations, which may be interpreted in different ways. While the FATF defined or explained some terms in the glossary or interpretive notes, 'suspicion' was not defined. It is worth mentioning that the 'suspicion' term was not clarified in the EU's Money Laundering Directive.[119] Moreover, neither recommendation 20 nor interpretive note to recommendation 20 explained what 'having reasonable grounds to suspect' means. Therefore, it is unclear whether **'**reasonable grounds to suspicion' should be understood as an objective test or a cumulative test covering objective and subjective tests. However, it is worth mentioning that suspicion'

---

[114] Interpretive Note to Recommendation 3, FATF (n.1), 38.
[115] Ibid.
[116] FATF website, 'High-risk and other monitored jurisdictions', <http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/more/more-on-high-risk-and-non-cooperative-jurisdictions.html?hf=10&b=0&s=desc(fatf_releasedate)> 10 June 2021.
[117] Interpretive Note to Recommendation 3, FATF (n.1), 38.
[118] Recommendation 1, FATF (n.1), 10.
[119] Article 33-1(a), 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.

and 'reasonable grounds to suspect' should be understood in compliance with recommendation 2. The FATF's recommendation 2 advises

> policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policymaking and operational levels …. to ensure the compatibility of AML/CFT/CPF requirements with Data Protection and Privacy rules and other similar provisions (e.g. data security/localisation).

However, the FATF officials have not yet explained what data protection and privacy rules to which recommendation 2 refers.

2.III.D. Financial institutions' duty of reporting and the FATF's recommendation 3

2.III.D.1. Introduction

The FATF, in its recommendation 3, advised countries to criminalise money laundering. In some countries where the FATF standards are given effect, one who failed to make an STR/SAR may be prosecuted with a money laundering offence. However, the FATF's recommendation 3 does not refer to the STRs/SARs.

2.III.D.2. Recommendation 3: The offence of money laundering

The FATF recommends countries to criminalise money laundering on the basis of the Vienna and Palermo Conventions.[120] According to the Vienna and Palermo Conventions, the offence of money laundering should apply to those who pursue a 'prohibited act' on 'criminal property' 'knowing that such property is criminal property'.[121]

According to Article 3(1) of the Vienna Convention and Article 6(1) of the Palermo Convention, the offence of money laundering should cover not only the acts of conversion, transfer, concealment and disguise[122] but also the acquisition, possession or use of the proceeds of a crime.[123] Besides, participation in, association or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of a money laundering offence should be criminalised.[124]

Interpretive Note to Recommendation 3 provides that "[t]he offence of money laundering should extend to any type of property, regardless of its value, that directly or indirectly represents the proceeds of

[120] FATF Recommendation 3, FATF (n.1), 12.
[121] Article 3(1) of the Vienna Convention, 1988 and article 6(1) of the Palermo Convention, 2000.
[122] Article 3(1)b of the Vienna Convention and Article 6(1)(a) of the Palermo Convention.
[123] Article 3(1)(c)(i) of the Vienna Convention and Article 6(1)(b)(i) of the Palermo Convention.
[124] 3(1)(c)(iv) of the Vienna Convention and Article 6(1)(b)(ii) of the Palermo Convention. See also FATF's Interpretive Note to Recommendation 3, para. 7-d.

crime."[125] Because AML laws should apply to "all forms of property, not just 'money' derived from criminal conduct", it is safe to defend that money laundering term is, in fact a misnomer.[126]

According to the FATF's Interpretive Note to Recommendation 3, "when proving that property is the proceeds of crime, it should not be necessary that a person be convicted of a predicate offence."[127]

The FATF recommends countries to "ensure that the intent or knowledge required to prove the offence of money laundering may be inferred from objective factual circumstances".[128] Hence, one who carries out a prohibited act on the criminal property while he knows or the objective factual circumstances show that he knows that it constitutes or represents criminal property should be prosecuted with a money laundering offence.

Punishment must be equal to the disturbance which it seeks to rectify.[129] According to the Interpretive Note to Recommendation 3[130], "[e]ffective, proportionate and dissuasive criminal sanctions should apply to natural persons convicted of money laundering."

Convicting any and all economic criminals (ie. an offender, real or legal person, who obtained acquisitive gain or advantage from its' criminal activity) who benefit from the proceeds of their crime of money laundering may lead to a double punishment problem. While the FATF advises countries to apply proportionate criminal sanctions,[131] the FATF officials did not explain the extent to which the offence of money laundering should apply to persons who committed the predicate offence. However, interpretive note to recommendation 3 highlighted that "[c]ountries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law".[132]

Criminal liability of corporations has been a sensitive issue for the FATF since its first-round recommendations.[133] The Interpretive Note to Recommendation 3 of the FATF Recommendations, updated October 2020, commented on the criminal liability of corporations as follows:[134]

> Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative

[125] Interpretive Note to Recommendation 3, FATF (n.1), 38.
[126] R Fortson QC, 'Money laundering offences under POCA 2002' in W Blair, R Brent and T Grant (eds), *Banks and financial crime – the international law of tainted money* (2nd edn, OUP 2017), 133.
[127] Interpretive Note to Recommendation 3, FATF (n.1), 38.
[128] Recommendation3, Interpretive Note to Recommendation 3, FATF (n.1), 38; Article 3(3) of the Vienna Convention and article 6(2)-f of the Palermo Convention.
[129] S P Brown, 'The moral justification of retributive punishment by reference to the notion of balance' (PhD thesis, University of Sheffield 1998), 190.
[130] Interpretive Note to Recommendation 3, FATF (n.1), 38.
[131] Ibid.
[132] Ibid.
[133] Recommendation 7, FATF (n.31).
[134] Interpretive Note to Recommendation 3, FATF (n.1), 38.

proceedings with respect to legal persons in countries in which more than one form of liability is available. Such measures should be without prejudice to the criminal liability of natural persons. All sanctions should be effective, proportionate and dissuasive.

2.III.D.3. The FATF's recommendation 3 and the STRs

In some countries where the FATF standards are given effect, one who failed to make a STR/SAR may be prosecuted with a money laundering offence. For instance, an English banker who failed to make an authorised disclosure may be prosecuted with a money laundering offence.[135] Similarly, a Swiss banker may be prosecuted with a money laundering offence where he failed to make a required disclosure under certain conditions.[136] Whilst, the FATF's recommendation 3, which advises countries to criminalise money laundering, does not refer to the SARs or STRs.

Recommendation 20 advises countries to impose upon financial institutions duty to play an active role in the fight against money laundering. According to the interpretive note, financial institutions' duty of reporting should be a direct mandatory obligation.[137] "Any indirect or implicit obligation to report suspicious transactions, whether by reason of possible prosecution for a money laundering or terrorist financing offence or otherwise" is not sufficient to comply with the requirements of recommendation 20.[138] Hence, financial institutions' duty of reporting should not be a mere extension of their duty not to commit a money laundering offence.

2.III.E. Recommendation 21: Rules that protect reporters from criminal and civil liability

The FATF advised countries to provide reporting persons with legal protection from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision.[139] "If they report their suspicions in good faith to the FIU", financial institutions, their directors, officers and employees should enjoy such legal protection "even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred"[140]. Hence, the FATF recommends countries to provide legal protection to the reporting persons where they "report in good faith".

[135] See pages 47-48.
[136] See page 78 .
[137] Interpretive Note to Recommendation 20, FATF (n.1), 87.
[138] Ibid.
[139] Recommendation 21, FATF (n.1), 19.
[140] Ibid.

The FATF officials did not further explain what 'reporting in good faith' means.[141] Until 2018, it was possible to understand this recommendation as meaning that not only but at least those who report in good faith should be protected by law from criminal and civil liability. In 2018, recommendation 2 advised policy makers and law enforcement agencies to ensure that AML measures comply with data protection and privacy laws. Because AML laws interfere with banking clients' information privacy rights by permitting financial institutions and their staff to make STRs, recommendation 21 should be interpreted in compliance with applicable information privacy laws. The FATF has not referred to any particular data protection and privacy rules or standards. Therefore, "data protection and privacy rules and other similar provisions" to which recommendation 21 referred should be understood as countries' national norms.

2.III.F. Recommendation 21: Prohibition of tipping off

The FATF, in its recommendation 29, advised countries to establish

> a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis.

The FIUs should use information disclosed by the banks in two ways[142]. First, they should use the SARs in initiating or conducting operational analysis

> to identify specific targets (e.g. persons, assets, criminal networks and associations), to follow the trail of particular activities or transactions, and to determine links between those targets and possible proceeds of crime, money laundering, predicate offences or terrorist financing. [143]

Second, the FIUs should use the SARs to identify money laundering related trends and patterns. [144] After identifying relevant trends and patterns, the FIUs can establish policies and goals for entities within the AML regime.[145] Hence, bankers' assessment in relation to the source origin of their clients' assets can help identify specific targets and increase the effectiveness of AML policy.

The FIUs need time to conduct their operational analysis. An offender who has been informed that a report was filed or provided with related information can carry out transactions that may reduce the success of following AML measures. For instance, the offender may withdraw criminal money or transfer it to a non-cooperative country.

[141] See Ibid. There is no interpretive note written to recommendation 21.
[142] Interpretive note to recommendation 29, FATF (n.1), 101.
[143] Ibid.
[144] Ibid.
[145] Ibid.

Tipping off rules aim to guarantee the success of the STRs regime. The FATF recommends countries to prohibit by law financial institutions and their staff "from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU". [146]

The FATF took measures to ensure that tipping off rules do not inhibit information sharing required for CDD and money laundering and terrorist financing risk management within a financial group.[147] According to the interpretive note to recommendation 18:

> Group-level compliance, audit, and/or AML/CFT functions should be provided with customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This should include information and analysis of transactions or activities which appear unusual (if such analysis was done); and could include an STR, its underlying information, or the fact that an STR has been submitted. Similarly, branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management. Adequate safeguards on the confidentiality and use of information exchanged should be in place, including to prevent tipping-off.

Tipping off rules are necessary but not sufficient for protecting the success of the STRs regime. First, the reported transaction might be a transaction that would make tracing paper trail of criminal money impossible. Second, banking staff involved in criminal conspiracy may still inform the criminals about the reports.[148] Some legal systems require the reporting person to freeze the reported client's bank account temporarily. However, the FATF did not recommend countries to require reporting persons to freeze the reported person's account or not to honour the reported client's mandate. This is understandable because most of the FIUs cannot analyse all the STRs/SARs they received within a reasonable time. In fact, most of the FIUs are not even able to analyse all the reports they received. Europol, in its 2017 report, established that, just 10% of the SARs in the EU were further investigated by the FIUs after collection and this figure was unchanged since 2006**.**[149]

2.III.G. Conclusion

This part showed that the FATF adopted recommendations open to different interpretations to advise countries to require and permit, by law, banks to make an STR where they suspect, or have reasonable grounds to suspect, that one of their client's funds constitute or represent proceeds of crime.

---

[146] Recommendation 21, FATF (n.1), 19.
[147] Ibid.
[148] A long list of cases have shown that money launderers take benefit from insiders at different levels. See F Hobson, 'Introduction: Banks and Money Laundering' in W Blair and R Brent (eds), *Banks and Financial Crime: The International Law of Tainted Money* (OUP 2008), 15. There are even cases where the bank was bought by the offenders. (See page 151 in chapter 4.) In a world where money launderers can buy banks, it would not be extreme to think that there can be banking staff who may provide information to offenders.
[149] Europol (n.10), 5.

2.IV. English AML laws

2.IV.A. Introduction

Financial institutions can increase their attractiveness by respecting their clients' privacy and secrecy. Conversely, they can lose existing or prospective clients where they fail to respect their clients' confidentiality. Therefore, secrecy culture in the banking business goes beyond and above bankers' legal duty of secrecy.[150]

In 1924, the Court of Appeal recognised banks' contractual duty of secrecy.[151] Prior to the *Tournier* rule, there was no clear authority on whether banks owe their clients a duty of secrecy.[152]

Banking professionals had been protecting their clients' confidentiality vigorously, even before the Court of Appeal's decision in *Tournier*.[153] One may easily find many 19th century cases relating to professionals' duty of confidentiality.[154] However, there were few bank secrecy related cases before 1924. Stokes,[155] Fowler and Butler,[156] Alpin et all[157] and Richardson et all[158] mention the following three cases only: *Tassell v Cooper* (1850),[159] *Foster v Bank of London* (1862)[160] and *Hardy v Veasey*

---

[150] Y Genier, *La fin du secret bancaire* **(**Savoir Suisse 2014), 36.

[151] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B. 461.

[152] W Fowler and R Butler, 'Great Britain' in D Campbell (ed), *International Bank Secrecy* (Sweet & Maxwell 1992), 243. Some 56 years before the Court of Appeal's decision in *Tournier*, Martin B, in *Hardy v Veasey* [1868] LR 3 Ex. 107, 112., put it that:

> I … should be sorry on the present occasion to pronounce an opinion, whether or not the law will imply a contract by a banker not to communicate the state of his customer's account except on a reasonable and proper occasion. There may be such a duty, but I confess I should like to see some authority in its support. It is one thing to be under a moral duty to do a thing, another to be bound by a contract. If the latter were made out, then the banker would be instantly liable for nominal damages on making the communication, though no injury whatever resulted. But if, from the relation between the banker and his customer, a duty is implied in the former, not to do any act to the damage of his customer, the position would be much easier to understand.

It is worth noting that Martin B, did not see the loss of secrecy of private facts as damage *per se*.

[153] Stokes (n.99), 5.

[154] Eg. A list of well-known cases relating to lawyer's duty of secrecy: *Beer v Ward* (1821) Jac 77, 37 ER 779; *Johnson v Marriott* (1833) 2 C & M 183, 149 ER 725; *Taylor v Blacklow* (1836) 3 Bing (NC) 235, 32 ER 401; *Davies v Clough* (1837) 8 Sim 262, 59 ER 105; *Lewis v Smith* (1849) 1 Mac & G 417, 41 ER 1326. For further investigation, see T Aplin et al., *Gurry on Breach of Confidence* (2nd ed, OUP 2012), [9.102].

[155] Stokes (n.99), 4-19.

[156] Fowler and Butler (n.152), 242-244.

[157] Aplin et al. (n.154), 2.66-2.81; 2.111-2.126.

[158] M Richardson et al, *Breach of Confidence: Social Origins and Modern Developments* (Edward Elgar 2011), 35-42.

[159] *Tassell v Cooper* (1850) 137 ER 990. In *Tassell v Cooper*, Baron De L'Isle and Dudley consulted the account book at the London & County Bank and found that their former farming bailiff Tassell had received and paid into his own account a cheque which belongs to the Baron. Tassell's council argued that the banker had a duty "not to expose or disclose the state or particulars of the said account so to be kept by them as aforesaid". (*Tassell v Cooper* (1850) 137 ER 990; (1850) 9 CB 509, 514.) The Court was ultimately not required to decide on this issue, because counsel agreed to abandon this count. It is worth mentioning that it was not all easy for Baron De L'Isle and Dudley to gain access to the account book. Baron De L'Isle and Dudley's request was initially declined by the branch manager of the London & County Bank.

[160] *Foster v Bank of London* (1862) 176 ER 96. *Foster v Bank of London* was a conspiracy case. Foster, who had given a cheque to De Roo & Co., had insufficient fund in his account in the Bank of London for the payment of

(1868).[161] As mentioned by Scrutton L.J., the fact that there is "so little authority as to the bankers' duty to keep customers, or clients' affairs secret" shows that bankers were motivated not to divulge their customer's banking data to third parties without the client's consent.[162]

While English bankers have a strong secrecy culture, AML laws adopted in the second half of the 20th century established an SARs regime bankers are making more than 400,000 reports per year.[163]

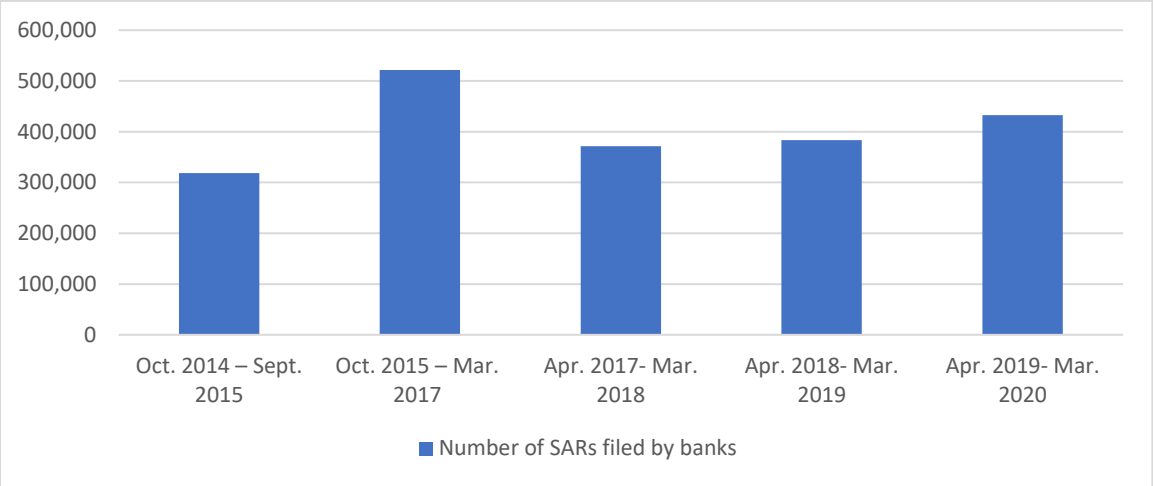


Chart 4: Number of SARs filed by banks in the UK.[164]

There are two types of suspicious activity reports that English bankers are required and permitted to make: authorised reports and required reports. One who fails to make an authorised disclosure may be prosecuted with a principal money laundering offence.[165] A banker who fails to make a required disclosure may be responsible for an ancillary money laundering offence.[166] Authorised and required

---

the cheque. De Roo & Co. learned from the banker exact amount of fund in Foster's bank account, and funded Foster's account as much as the cheque becomes payable. Channell B, in *Hardy v Veasey* (1868) LR 3 Ex. 107, 113., commented on Foster case as follows:

> The case cited of Foster v. Bank of London (citation omitted), seems correct; and if the observations of the chief justice are taken in connection with the facts of that case, there is no ground to complain of them, but they do not, I think, support the plaintiff's argument. It was not so much there the case of a disclosure of the customer's account, as of a trick, by which the bank conspired with one of the plaintiff's creditors to the prejudice of the rest; and the language of the chief justice is guarded, for he says emphatically that he knows of no law against the action being maintainable.

[161] *Hardy v Veasey* [1868] LR 3 Ex. 107.

[162] *Tournier v. National Provincial and Union Bank of England* (1924)1 KB 461, at 479 (by Scrutton L.J.).

[163] See National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2020', 2020, 11.

[164] This chart was prepared by using information provided in the UKFIU's Annual reports 2020, 2019, 2018, 2017, 2015. See National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2020', (2020), 9; National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2019', (2019), 8; National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2018', (2018), 6; National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2017', (2017), 12; and National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2015', (2015), 9.

[165] See sections 327-329 and 338 of POCA 2002.

[166] See sections 330 and 331 of POCA 2002.

disclosures are "not to be taken to breach any restriction on the disclosure of information"[167]. Moreover, AML laws prohibited tipping off.[168]

2.IV.B. Defence against Money Laundering Suspicious Activity Reports

One who fails to make an appropriate authorised disclosure may commit a money laundering offence and may be prosecuted with a jail term up to 14 years or to a fine or to both.[169]

2.IV.B.1. The offence of money laundering

Part 7 of POCA 2002 specifies eight offences, while section 340(11) of the Act recognises only three of them (ie. Concealing etc. in section 327, arrangements in section 328 and acquisition, use and possession in section 329) as money laundering offences. Five others (ie. failure to disclose and tipping off offences in sections 330-333A) are ancillary to the principal money laundering offences.[170] Therefore, money laundering offences are separated into two groups in English literature: principal and ancillary money laundering offences.[171] It is worth mentioning that the ancillary offences term has been used in a different meaning in the FATF's Interpretive Note to Recommendation 3, paragraph 7-d, where participation in, association with or conspiracy to commit, attempt, aiding and abetting, facilitating, and counselling the commission of money laundering are listed as examples of ancillary offences to the offence of money laundering.

2.IV.B.1.a. Prohibited act

One commits a money laundering offence:[172]
(a) if he (i) conceals[173] or disguises[174] criminal property, its' nature, source, location, disposition, movement or ownership or any rights with respect to it;[175] (ii) converts[176] or transfers[177] criminal

[167] Sections 337-1 and 338-4, POCA 2002.
[168] Section 333(A) of POCA 2002.
[169] See sections 327,328,329 and 338 of POCA 2002.
[170] Fortson QC (n.126), 139.
[171] M Sutherland Williams, M Hopmeier and R Jones, *Millington and Sutherland Williams on the Proceeds of Crime* (4th ed, OUP 2013, 509.
[172] See sections 340(11), 327(1), 328(1) and 329(1) of POCA 2002.
[173] Section 327 (1)-a, POCA 2002.
[174] Section 327 (1)-b, POCA 2002.
[175] Section 327 (3), POCA 2002.
[176] Section 327 (1)-c, POCA 2002.
[177] Section 327 (1)-d, POCA 2002.

property, (iii) removes criminal property from England and Wales or from Scotland or from Northern Ireland[178] *(Section 327-1)*, (iv) enters into or becomes concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person *(Section 328-1)*, (v) acquires[179] or uses[180] criminal property; or (vi) has possession[181] of criminal property *(Section 329-1)*,

(b) if his act constitutes an attempt, conspiracy or incitement to commit any of the above-specified offences (*section 340 (11)-b*),

(c) if his act constitutes aiding, abetting, counselling or procuring the commission of an offence above specified (*section 340 (11)-c*), or

(d) if his act would constitute an offence specified in paragraphs (a), (b) or (c) if done in the United Kingdom (*section 340 (11)-d*).

POCA 2002 criminalised money laundering in compliance with the Vienna and Palermo Conventions and the FATF's recommendations.[182]

There are some exemptions recognised in sections 327, 328 and 329 of POCA 2002. First, a person does not commit such an offence if he makes an appropriate authorised disclosure.[183] Second, a deposit-taking body, electronic money institution or payment institution does not commit such an offence if it converts or transfers money in operating an account maintained with it, and the value of the criminal property concerned is less than £250.[184] Third, a person does not commit such an offence if the act he does is done in carrying out a function he has relating to the enforcement of any provision of POCA 2002 or of any other enactment relating to criminal conduct or benefit from criminal conduct.[185] The burden of proving that any of the exemptions listed in the sections do not apply stays on the prosecution.[186] Lastly, a person does not commit an offence under section 329 if "he acquired or used or had possession of the property for adequate consideration"[187].

[178] Section 327 (1)-e, POCA 2002.
[179] Section 329 (1)-a, POCA 2002.
[180] Section 329 (1)-b, POCA 2002.
[181] Section 329 (1)-c, POCA 2002.
[182] FATF (2018) (n.90), 176-177
[183] Sections 327 (2), 328 (2) and 329 (2), POCA 2002.
[184] Sections 327 (2C), 328 (5) and 329 (2C), POCA 2002. The threshold amount is determined under section 339A of the Act.
[185] Sections 327 (2), 328 (2) and 329 (2), POCA 2002.
[186] Sutherland Williams, et all (n.171), 516 at 20.50.
[187] Sections 329(2)-(3).

2.IV.B.1.b. Criminal property

According to section 340(3) of POCA 2002, one's benefit from criminal conduct or any asset representing such benefit (in whole or part and whether directly or indirectly) constitutes criminal property if the alleged offender knows or suspects that it constitutes or represents such benefit. Hence, any property or pecuniary advantage may be qualified as criminal property if the following two conditions are met: (i) it constitutes or represents one's benefit from criminal conduct and (ii) the alleged offender knows or suspects that it constitutes or represents such benefit. The alleged offender in condition ii and the author of the criminal conduct in condition i can be the same person or different persons.

2.IV.B.1.b.i. Condition-1. One's 'benefit' from 'criminal conduct' or any asset which represents such benefit

Benefit. 'Benefit from criminal conduct' covers both property and pecuniary advantage obtained as a result of or in connection with the criminal conduct.[188] The money laundering offences extend to any property wherever situated, regardless of its value, and includes not only money but also all forms of property.[189] However, it is worth mentioning that a deposit-taking body, electronic money institution or payment institution does not commit a money laundering offence if it converts or transfers money in operating an account maintained with it, and the value of the criminal property concerned is less than £250.[190]

Criminal Conduct. POCA 2002 prescribes predicate offences by reference to all offences. Indeed, according to section 340(2) of POCA 2002, conduct that constitutes an offence in any part of the UK constitutes criminal conduct. Hence, one's benefit from conduct which constitutes an offence in any part of the UK or any asset which represents such benefit (in whole or part and whether directly or indirectly) constitutes criminal property if the second condition (the alleged offender knows or suspects that it constitutes or represents such benefit) is also met.[191] Therefore, English law is assessed compliant with Criterion 3.2 in the FATF's 2018 Mutual Evaluation Report.[192]

[188] See sections 340(5) and 340(6) of POCA 2002. In relation to 'pecuniary advantage', see R v Smith [2001] UKHL 68; R v Foggom [2003] EWCA Crim 270; R v Bowbotham [2006] EWCA Crim 747; R v Homer [2006] EWCA Crim 1559; R v IK [2007] EWCA Crim 491; R v Gabriel [2006] EWCA Crim 229.
[189] Section 340 (9), POCA 2002.
[190] Sections 327 (2C), 328 (5), 329 (2C) and 339A, POCA 2002.
[191] Section 340 (3), POCA 2002.
[192] FATF (2018) (n.90), 177.

English financial system is attractive for assets derived from offences that are committed abroad.[193] For the purposes of section 340(2) of POCA, it is irrelevant whether the predicate offence was committed abroad as long as this conduct would constitute an offence if it occurred in the UK. However, the legislator acknowledged that this might be unfair to those who lawfully gained money in another jurisdiction and brought their money into the UK, where their conduct is illegal. An often-cited example is the situation of a matador lawfully working in Spain and investing in the UK, where bullfighting is unlawful.[194] This issue is solved with a general exemption recognised for all principal and ancillary money laundering offences. A person does not commit a money laundering offence, if

> (a) he knows, or believes on reasonable grounds, that the relevant criminal conduct occurred in a particular country or territory outside the United Kingdom, and
>
> (b) the relevant criminal conduct (i) was not, at the time it occurred, unlawful under the criminal law then applying in that country or territory, and (ii) is not of a description prescribed by an order made by the Secretary of State.[195]

According to the Proceeds of Crime Act 2002 (Money Laundering: Exceptions to Overseas Conduct Defence) Order (SI 2006/1070), all criminal conduct is prescribed if it would constitute an offence punishable by imprisonment for a maximum term of twelve months, if it was occurred in any part of the UK, and if it is a crime under the Gaming Act 1968, the Lotteries and Amusement Act 1976, sections 23 or 25 of the Financial Services and Markets Act 2000.

According to section 340(3) of POCA, there is no requirement that a person be convicted of a predicate offence to prove that property is the proceeds of crime. The prosecution should prove that property derives from criminal conduct and show the type of criminal conduct.[196] The Court of Appeal, in *R v Anwoir*, submitted that[197]

> there are two ways in which the Crown can prove the property derives from crime, (a) by showing that it derives from conduct of a specific kind or kinds and that conduct of that kind or those kinds is unlawful, or (b) by evidence of the circumstances in which the property is handled which are such as to give rise to the irresistible inference that it can only be derived from crime.

Therefore, English law complies with paragraph 4 of the FATF's Interpretive Note to Recommendation 3.[198]

---

[193] FATF (2018) (n.90), 18.
[194] Fortson QC (n.126), 180.
[195] Sections 327 (2A), 328 (3), 329 (2A), 330 (6), 331 (6A) and 332 (7), POCA 2002.
[196] *R v W and C* [2008] EWCA Crim 2, [2009] 1 WLR 965, [2008] 3 All ER 533, [2008] Lloyd's Rep FC 163, [2008] Crim LR 900. For further information, see Fortson QC (n.126), 146.
[197] [2008] EWCA Crim 1354 at [21].
[198] FATF (2018) (n.90), 177.

2.IV.B.1.b.ii. Condition-2: The alleged offender knows or suspects that it constitutes or represents such benefit

The UK went beyond the requirements of the Vienna and Palermo Conventions.[199] One's benefit from criminal conduct or any asset which represents such benefit constitutes criminal property if the alleged offender knows or suspects that it constitutes or represents such benefit.[200] One who carries out a prohibited act on the criminal property knowing or suspecting that such property is or represents proceeds of a crime commits a money laundering offence unless he makes an appropriate authorised disclosure.[201] It is worth mentioning that *mens rea* applicable for the offence of conspiring to launder criminal property is not suspicion, knowledge or intention is required[202].

There is no statutory definition of the term 'suspicion', which is an ordinary word of the English language.[203] According to a general principle of statutory interpretation in criminal law endorsed by the House of Lords in Brutus v Cozens, "the meaning of an ordinary word of the English language is not a question of law".[204] The Court of Appeal, in *R v Da Silva*, "re-iterated that a trial judge could not be criticised if he or she did not define suspicion for the jury other than to say it was an ordinary English word and the jury should apply their own understanding of it."[205] However, "a judge was not precluded from offering more assistance to the jury."[206] The Court of Appeal explained the meaning of the word 'suspicion' in section 93A of the Criminal Justice Act 1988 as follows:[207]

> It seems to us that the essential element in the word "suspect" and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice. But the statute does not require the suspicion to be "clear" or "firmly grounded and targeted on specific facts", or based upon "reasonable grounds". … We consider therefore that, for the purpose of a conviction under section 93A(1)(a) of the 1988 Act, the prosecution must prove that the defendant's acts of facilitating another person's retention or control of the proceeds of criminal conduct were done by a defendant who thought that there was a possibility, which was more than fanciful, that the other person was or had been engaged in or had benefited from criminal conduct.

---

[199] *R v Montila* [2004] 1 W.L.R. 3141 at [38]; FATF (2018) (n.90), 177 at [3.8].
[200] Section 340 (3), POCA 2002.
[201] Sections 327 (2), 328 (2) and 329 (2), POCA 2002.
[202] Section 1(2) of the Criminal Law Act 1977 and sections 327, 328 and 329 of POCA 2002. See R v Saik [2007] 1 AC 18 and R v Thomas [2014] EWCA Crim 1958. Similarly, in relation to attempts to commit a money laundering offence, see section 1 of the Criminal Attempts Act and R v Pace [2014] EWCA Crim 186. For a further discussion see Fortson QC (n.126), 152.
[203] *R v Da Silva* [2006] EWCA Crim 1654 at [16].
[204] *Brutus v Cozens* (1972) 56 Cr. App. R. 799, 804.
[205] Law Commission (n.5), [6.20], [6.41].
[206] Ibid, [6.41].
[207] *R v Da Silva* [2006] EWCA Crim 1654 at [16].

Hence, suspicion is an ordinary word and does not need a statutory definition. If explained, "one who suspects" in sections 327 to 329 of POCA 2002 means that one who thinks that there is a possibility, which is more than fanciful, that the other person was or had been engaged in or had benefited from criminal conduct. The definition of suspicion in *R v Da Silva* has been confirmed in following cases.[208]

English law is unique in accepting the low threshold of suspicion.[209] Punishing one who pursues a prohibited act on the assets he suspects are or represent criminal property without making an authorised disclosure is criticised largely in literature. Some authors defend that suspicion is a vague term and needs to be defined or further clarified.[210] Some others go further, arguing that suspicion is an excessively low threshold for principal money laundering offences.[211]

2.IV.B.1.c. Sanctions

Principal money laundering offences specified in sections 327, 328 and 329 of the POCA 2002 can be categorised as serious crimes.[212] According to section 334-1(b) of POCA 2002, a person guilty of one of the three principal money laundering offences "is liable (a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both, or (b) on conviction on indictment, to imprisonment for a term not exceeding 14 years or to a fine or to both".

The FATF, in its interpretive note to recommendation 3 established that "[c]ountries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law".[213] Whilst, the perpetrator of the predicate offence, may be sentenced for a money laundering offence in the UK[214].

The ambit of sections 327 and 329 of POCA 2002 is wide. Indeed, English AML laws criminalised even mere use or possession of the criminal property. These sections may lead the prosecution to lay

[208] *K Ltd v National Westminster Bank* [2006] EWCA Civ 1039 at [16]; and *Shah v HSBC* [2012] EWHC 1283.
[209] Response of the Law Society of England and Wales to the consultation issued by the Home Office and HM Treasury on the Action Plan for anti-money laundering and counter-terrorist finance – legislative proposals (June 2016) in Law Commission (n.5), [14.4].
[210] P Marshall, 'Does Shah v HSBC Private Bank Ltd make the anti-money laundering consent regime unworkable?'' May 2010, Butterworths Journal of International Banking and Financial Law 287, 289; G Brown and T Evans, 'The impact: the breadth and depth of the anti-money laundering provisions requiring reporting of suspicion activities' (2008) Journal of International Banking Law Regulations 274, 275.
[211] D Ormerod and K Laird, *Smith, Hogan, and Ormerod's Criminal Law* (15th ed, OUP 2018), at [3.2.8.]; Law Commission, Anti-money laundering: the SARs regime (Law Com No 384, 2019), [5.11].
[212] S F Preller, 'Comparing AML legislation of the UK, Switzerland and Germany, (2008) 11(2) J.M.L.C. 234, 236.
[213] Interpretive Note to Recommendation 3 (Money laundering offence), at [6].
[214] Section 340(4) of POCA. See R v Greaves and others [2010] EWCA Crim 709, at [24].

additional charges to the perpetrator of the predicate offence.[215] It is worth mentioning that one who is charged under sections 327 and 328 of POCA 2002 faces additional punishment and may be subject to stronger confiscation provisions.[216] Latham LJ in *R v Allpress* rightly established that[217]

> it would be unsatisfactory if a result of the prosecution choosing to lay a charge under POCA 2002, s329, the confiscation provisions of the Act would apply differently than if on the same facts the offender had been charged with burglary or handling stolen property.

These concerns led to an important question: when the prosecution should add additional counts on the basis of sections 327 and 329 to a defendant who is also indicted for the underlying offence? The UK Supreme Court, in *R v GH*[218], clarified this issue as follows:

> [I]t would be bad practice for the prosecution to add additional counts *[under sections 327 and 329]* unless there is a proper public purpose in doing so, for example, because there may be doubt whether the prosecution can prove that the defendant was the thief but it can prove that he concealed what he must have known or suspected was stolen property, or because the thief's conduct involved some added criminality not just as a matter of legal definition but sufficiently distinct from the offence that the public interest would merit it being charged separately…..The courts should be willing to use their powers to discourage inappropriate use of the provisions of POCA to prosecute conduct which is sufficiently covered by substantive offences.

The Crown Prosecution Service's relevant guidance is in line with the Supreme Court's position. It clearly stated that "[t]he prosecutor should take into account whether the laundering activity involves such a significant attempt to conceal ill-gotten gains that a court may consider a consecutive sentence".[219] Hence, the Courts took measures against double punishment.

The Court of Appeal explained the relation between the maximum sentence permitted on the predicate offence and the sentence on the offence of money laundering as follows:[220]

> Where the conduct involved in the Proceeds of Crime Act offence does add to the culpability of the conduct involved in the primary offence, the maximum sentence permitted on the primary offence may be relevant to the sentence on the Proceeds of Crime Act offence because the seriousness of the primary offence reflects on the seriousness of

[215] [2009] EWCA Crim 8, para 44 *per* Latham LJ. Similar concerns were expressed by Maurice K LJ in *R(Wiklinson) v Director of Public Prosecutions* [2006] EWHC 3012 (Admin) at [8], and by Richards LJ in *CPS Nottinghamshire v Kevin Rose* [2008] EWCA Crim 239, at [19] and [20].
[216] Eg. see sections 75(1)-(2) of POCA and Money Laundering in Schedule 2.
[217] *R v Allpress* [2009] EWCA Crim 8 at [44] *per* Latham LJ.
[218] *R v GH* [2015] 1 WLR 2126 at [48] and [49] *per* Lord Toulson JSC. See similar arguments from the Court of Appeal in R v Greaves and others [2010] EWCA Crim 709, at [24]; and R v Alexander and others [2011] EWCA Crim 89 at [11].
[219] CPS, 'Proceeds Of Crime Act 2002 Part 7 - Money Laundering Offences', Legal Guidance, <https://www.cps.gov.uk/legal-guidance/proceeds-crime-act-2002-part-7-money-laundering-offences> 13 August 2020.
[220] *R. v Claude Clifford Greaves and Others* [2010] EWCA Crim 709, [24].

> the laundering: see, for instance, *R v Greenwood* [[1995] 16 Cr App R (S) 614] and *R v Basra* [[2002] EWCA Crim 541]. But it does not as a matter of principle provide a limit: see *R v Linegar* [[2009] EWCA Crim 648] . If the Proceeds of Crime Act offence merits it, the sentence for it may add to that for the primary offence bringing it above the maximum for the latter, and it may if appropriate itself exceed the maximum on the latter: see *R v Linegar* [[2009] EWCA Crim 648].

According to the FATF's Interpretive Note to Recommendation 3 "[c]riminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons."[221] A legal person can be convicted and sentenced of a money laundering offence in the UK if both *actus reus* and *mens rea* are proven.[222] In a corporate context, any of the company's employees or agents can commit *actus reus*.[223] Whilst, the *mens rea* must be found amongst the "directing mind and will of the company".[224] According to the identification principle, a company can be liable for a money laundering offence if a senior corporate officer is involved in the offence.[225] This provides extreme protection for large companies such as banks.[226]

The UK legislator adopted some failure to prevent offences. The first one was the offence of a failure of commercial organisations to prevent bribery recognised in section 7 of the Bribery Act. The commercial organisation is guilty of an offence under section 7 where employees or agents engage in conduct that would amount to a bribery offence, unless the commercial organisation can show that they have in place 'adequate procedures designed to prevent' such conduct. Similarly, Criminal Finances Act 2017 adopted two failure to prevent offences: "Failure to prevent facilitation of UK tax evasion offences"[227] and "Failure to prevent facilitation of foreign tax evasion offences"[228]. However, there is no failure to prevent money laundering offence yet.[229]

---

[221] Interpretive Note to Recommendation 3 (Money laundering offence), at [7].
[222] *Tesco Supermarkets Ltd v Nattrass* [1972] AC 153
[223] *Tesco Supermarkets Ltd v Nattrass* [1972] AC 153
[224] *Lennard v Asiatic Petroleum* [1915] AC 705 at 715.
[225] S Montagu-Cairns, 'Corporate criminal liability and the failure to prevent offence: an argument for the adoption of an omissions-based offence in AML' in K Benson, C King and C Walker (eds) *Assets, Crimes, and the State - Innovations in 21st Century Legal Responses* (Routledge 2020), 87.
[226] Ibid and C Wells, *Corporations and Criminal Responsibility* (2nd ed, Oxford University Press 2001), chap. 5.
[227] Section 45, POCA 2002.
[228] Section 46, POCA 2002.
[229] There was a proposal to adopt a failure to prevent offence for money laundering during a House of Lords stage of the Sanctions and Anti-Money Laundering bill, but this proposal was not accepted. (Hansard (House of Lords) vol. 637, cols. 156, 157 6 March 2018.) In 2017, the Ministry of Justice issued a call for evidence which was "concerned with criminal offences designed to punish and prevent economic crimes such as fraud, false accounting and money laundering when committed on behalf or in the name of companies". See Ministry of Justice, Corporate Liability for Economic Crime Call for evidence, January 2017, <https://consult.justice.gov.uk/digital-communications/corporate-liability-for-economic-crime/supporting_documents/corporateliabilityforeconomiccrimeconsultationdocument.pdf> 10 June 2021.

2.IV.B.2. DAML SARS and the offence of money laundering

2.IV.B.2.a. Bankers' duty of reporting

According to the Vienna and Palermo Conventions, the offence of money laundering should apply to those who pursue a prohibited act on criminal property, knowing that such property is criminal property.[230] The FATF recommends countries to "ensure that the intent or knowledge required to prove the offence of money laundering may be inferred from objective factual circumstances".[231] As explained above, English law exceeded the requirements of the UN Conventions and the FATF recommendations. According to sections 327 (Concealing etc.), 328 (Arrangements), and 329 (Acquisition, use and possession) of POCA 2002, one commits a money laundering offence if he pursues a prohibited act (eg. converting, transferring, concealing, controlling etc.) on assets he knows or suspects that constitute or represent benefit from criminal conduct[232]. A banker who provides financial service to its' criminal client[233] commits a money laundering offence if they know or suspect that the client's funds are or represent criminal money. This creates an essential risk for banks and their staff, as one who commits a money laundering offence may be prosecuted with a jail term of up to 14 years or to a fine or to both.[234]

While English law recognized a remarkably low threshold, 'suspicion,' as sufficient for the mental element of the offence,[235] it also established a new mechanism: authorized reports or consent reports.[236] A person does not commit a money laundering offence if;

The consultation was issued to consider the extension of the Bribery Act failure to prevent model offence to a wider range of economic crimes. (Ibid, 8.) However, there is no bill drafted yet.

[230] Article 3.1, the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention 1988); article 6.1, the United Nations Convention against Transnational Organized Crime (Palermo Convention 2000) and the FATF Recommendation 3, *Money laundering offence*.

[231] FATF, Interpretive Note to Recommendation 3, *Money laundering offence*, [7]; Article 3.3, Vienna Convention 1988 and article 6.2, Palermo Convention 2000.

[232] Section 340 (3), POCA 2002.

[233] In common law, one may be accepted as a customer of a bank if he has an account in the bank. Lord Dunedin, in *Commissioners of Taxation v English, Scottish and Australian Ltd.*, observed that "[t]he contrast *[between a customer and a non-customer user]* is not between an habitué and a new comer, but between a person for whom the bank performs a casual service, such as, for instance, cashing a cheque for a person introduced by one of their customers, and a person who has an account of his own at the bank." (*Commissioners of Taxation v English, Scottish and Australian Ltd.* [1920] AC 83 (687).) The HM Treasury, in 2007, in relation to the now revoked Regulations 2007, stressed that for AML/CTF purposes "'customer' is to be interpreted as including the clients of professionals" (HM Treasury, 'Money Laundering Regulations 2007: Summary of Responses to consultation on draft Regulations' July 2007, [3.5]). There is no reason to think that the HM Treasury's relevant interpretation changed when the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 was adopted.

[234] Section 334(1), POCA 2002.

[235] *R v Da Silva* [2006] EWCA Crim 1654, at [16]-[17]; Ormerod and Laird (n.210), [3.2.8].

[236] Early examples of the authorised reports regime may be found in Section 24(3) of Drug Trafficking Offences Act 1986 and section 93(A) of Criminal Justice Act 1998.

(a) he makes an authorised disclosure under section 338 and (if the disclosure is made before he does the act mentioned in subsection (1)) he has the appropriate consent;

(b) he intended to make such a disclosure but had a reasonable excuse for not doing so.[237]

This means that a banker who made an authorised disclosure can provide service to its client without committing a money laundering offence, even where he knows or suspects that the property of the client is or represents criminal property. If the banker made the disclosure before he pursues the prohibited act, he should wait for the appropriate consent. Appropriate consent in sections 327 to 329 of POCA 2002 means "consent to do a prohibited act following an authorised disclosure."[238] Consent may relieve the reporting person "of any criminal responsibility for a transaction in question; but that does not mean that in relation to others involved in the transaction, it may not amount to or form part of a dishonest money-laundering scheme".[239]

The UKFIU uses Defence Against Money Laundering Suspicious Activity Reports (DAML SARs) and Defence Against Terrorist Financing Suspicious Activity Reports (DATF SARs) terms rather than authorised reports or consent reports terms[240], aiming to educate reporters and improve submissions by clarifying what the UKFIU can and cannot grant.[241]

Suspicion. As explained above, 'suspicion' is an ordinary word of the English language[242] and "the meaning of an ordinary word of the English language is not a question of law".[243] Therefore, there is no statutory definition of the term 'suspicion'.

AG Sharpston explained what should be understood from suspicion term used in the Money Laundering Directive as follows:[244]

> The Money Laundering Directive does not define 'suspicion of money laundering or terrorist financing'. Although Article 22(1)(a) (on the scope of the obligation to report to the FIU) suggests that having 'suspicion' is not the same as having 'reasonable grounds to suspect' that money laundering or terrorist financing is being (or has been) committed or attempted. I consider that that distinction cannot be read to mean that 'suspicion' in Article 7(c) is a purely subjective matter. In my opinion, suspicion must be based on some objective material that is capable of review in order to verify compliance with Article 7(c) and other provisions of the Money Laundering Directive. Thus, in my opinion, 'a suspicion

[237] Sections 327(2), 328(2) and 329(2), POCA 2002.
[238] Law Commission (n.5), [2.79].
[239] *AP, U Limited v CPS, RCPO* [2007] EWCA Crim 3128, at [32].
[240] Eg. see National Crime Agency, UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2017, 4.
[241] Law Commission (n.5), 2.11.
[242] *R v Da Silva* [2006] EWCA Crim 1654 at [16].
[243] *Brutus v Cozens* (1972) 56 Cr. App. R. 799, 804.
[244] Opinion of AG Sharpston, Case C-235/14 Safe Interenvios, SA v Liberbank, SA; Banco de Sabadell, SA and Banco Bilbao Vizcaya Argentaria, SA Official Journal of the European Union, C 235, Vol. 57, 21 July 2014, para 128.

> of money laundering or terrorist financing' within the meaning of Article 7(c) of Directive 2005/60 arises in particular where, taking into account the individual circumstances of a customer and his transactions (including with respect to the use and management of his account(s)), there are some verifiable grounds showing a risk that money laundering or terrorist financing exists or will occur in relation to that customer.

The Court of Appeal's explanation of suspicion in *R v Da Silva* seems to be in compliance with Advocate General Sharpston's opinion in Case C-235/14.

In *Michaud v France*, a case where lawyers' duty of reporting their money laundering and terrorist financing suspicions was challenged, the applicant argued that the term "suspicions" was not defined and constituted a breach of the requirement of legal certainty.[245] The European Court of Human Rights (ECtHR) rejected this claim considering that "the notion of "suspicions" is a matter of common sense and that an informed group such as lawyers can scarcely claim that they do not understand it in that … the Monetary and Financial Code gives specific guidance.".[246] English authorised reports regime differs in two points. First, there is no general guidance explains what suspicion means for sections 327 to 329. Second, sections 327 to 329 of POCA 2002 apply to everyone, not only an informed group of people.

As mentioned above, no guidance defines or explains what suspicion means for sections 327 to 329. However, it is worth looking at the Guidance mentioned in the ECtHR's decision. The guidance mentioned in the decision explains the term 'suspects' as follows:[247]

> There is no legal definition of suspicion. To understand the term "suspect", it could be helpful to refer to the interpretation of the Conseil d'Etat in its Judgment of 31 March 2004, which was handed down under the old regulations. This judgment states that, if the information gathered by an investment undertaking, in accordance with due diligence under the applicable regulations, does not let the undertaking rule out any suspicion about the lawfulness of the transaction or the origin of the sums involved, and thus rule out the possibility that these sums are the proceeds of an underlying offence, it must file a report with Tracfin.

If this is enough guidance, the explanation of suspicion provided in *R v Da Silva* should also be enough as guidance.

Some defend that 'suspicion' is an 'ill-defined and unclear' threshold and argue that the financial sector is producing a high volume of unwarranted reports due to the lack of definition of the term suspicion.[248]

---

[245] Michaud v France (2014) 59 E.H.R.R. 9, at [15].
[246] Michaud v France (2014) 59 E.H.R.R. 9, at [24].
[247] Autorite Des Marches Financiers, *'Guidelines on the obligation to report suspicious transactions to TRACFIN'* (2010).
[248] See Law Commission (n.5), [4.16], [6.7]; Law Commission (n.211), [5.37]; P Alldridge, *What Went Wrong with Money Laundering Law* (1st ed, Macmillan Publishers 2016), 38; and Law Commission (n.210), [5.37] ,[5.44], [5.46], [5.47].

Therefore, they suggest that suspicion should be defined. For instance, the Association of Accounting Technicians submitted that "As a result of the current lack of definition it is likely, indeed inevitable, that the quality and consistency of reporting is being affected."[249] The Crown Prosecution Service also argued for a statutory definition for suspicion. They submitted that[250]

> Given the spectrum of potential definitions and a variance in how persons interpret and understand this concept…a statutory definition would assist. That is particularly so in shaping how reporters may be required to express and explain the report they make. We would deprecate the suggestion that suspicion is a "feeling" and cannot be defined more clearly than this. [251]

While the Crown Prosecution Office assessed that "shaping how reporters may be required to express and explain the report they make" may be achieved by making a statutory definition,[252] it is worth noting that section 339(1) prescribes that "the Secretary of State may by order prescribe the form and manner in which a disclosure under section 330, 331, 332 or 338 must be made."[253]

This thesis defends that 'suspicion' is not an ill-defined or unclear threshold.[254] Those who defend that there exist unwarranted reports because suspicion has no statutory definition, fail to distinguish following two questions: (1) "What do we mean by suspicion?" (2) "Under what conditions should one suspect that another person was or had been engaged in or had benefited from criminal conduct?". The answer to the first question can be given by defining or explaining the suspicion term. The answer to the second question, on the other hand, can be given by providing training on money laundering methods and risk factors.

What do we mean by suspicion? Suspicion is an ordinary English word, and "an ordinary English word should only be defined where it is to be qualified in some way or given special meaning".[255] There is no reason to defend that suspicion is used in sections 327 to 329 of POCA 2002 in a special meaning.[256] Defining an ordinary word in status comes with some problems. The Law Commission asked consultees whether suspicion should be defined, and twenty-seven responses out of thirty-six agreed that defining suspicion would be problematic, pointing out the difficulty and repercussions of defining an ordinary word .[257] For instance, Slaughter and May observed that: "…attempting to define what is a normal

[249] Ibid ,[5.46].
[250] Ibid ,[5.45].
[251] Ibid ,[5.45].
[252] Law Commission (n.211), [5.37], [5.45].
[253] Section 339(1), POCA 2002.
[254] For a similar opinion submitted by Corruption Watch, see Law Commission (n.211), [5.41].
[255] *Brutus v Cozens* (1972) 56 Cr. App. R. 799, 804. Law Commission (n.5), 9.5.
[256] *R v Da Silva* [2006] EWCA Crim 1654 at [16].
[257] Law Commission (n.211), [5.41].

English word may leave potential reporters in a difficult position where they may feel suspicious in the ordinary sense of but not meet the elements of the definition."[258]

"Under what conditions one should suspect that another person was or had been engaged in or had benefited from criminal conduct?" One's capacity to distinguish regular, unusual and suspicious activities depends on their knowledge of money laundering methods and risk factors. The JMLSG Guidance explains the difference between unusual and suspicious transactions as follows:[259]

> A transaction which appears unusual is not necessarily suspicious. Even customers with a stable and predictable transactions profile will have periodic transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of transactions or account activity. So the unusual is, in the first instance, only a basis for further enquiry, which may in turn require judgement as to whether it is suspicious.

One who does not know what factors may show that the funds are likely to be criminal money cannot distinguish unusual and suspicious transactions.

Those who cannot distinguish unusual and suspicious transactions tend to be overcautious and produce unnecessary reports. The lack of training may be what leads to over-reporting. This argument may be supported by examining one of the unwarranted disclosure examples given by the Law Commission, which reads as follows: [260]

> A British professional of minority ethnic origin arranged a transfer of funds to purchase a property. The funds were being sent from their parents' country of origin and documentation as to the source of the funds had been provided. The reporter lodged an authorised disclosure on the basis that they had never dealt with a transaction from the relevant country before and therefore made a report out of caution.

This transaction was an unusual transaction from the perspective of the reporter in the sense that the funds came from a country from which the reporting person had never dealt with a transaction before. To analyse whether this unusual transaction amounts to a suspicious transaction, one should know money laundering methods and risk factors that show that one is laundering proceeds of crime or the funds are proceeds of crime. For instance, the person who is to analyse such unusual transaction should be aware of the loan back schemes and money launderers' use of the UK property market[261], and offshore states in such schemes to analyse whether he/she should make a disclosure where he/she faces such an unusual transaction. If the country from which the funds came was an offshore country and the transaction at stake had particularities that made it look like part of a loan-back scheme, the relevant

[258] Law Commission (n.211), [5.42].
[259] JMLSG, Prevention of Money Laundering, 2009, [6.12].
[260] Law Commission (n.2110), 97.
[261] Z Rodionova, 'London property market turned into money laundering safe haven by inadequate supervision, MPs say', The Independent, 15 July 2016 <https://www.independent.co.uk/news/business/news/london-property-market-real-estate-money-laundering-overseas-foreign-buyers-mps-a7138176.html> 10 June 2021.

person should have found the transaction suspicious. If the person does not know whether or not such a situation corresponds to a money laundering method or involves money laundering risk factors, they may be tempted to making a disclosure "out of caution". However, this is by no means that that person does not understand what suspicion means. In this example, it is hard to defend that the reporting person argues that "I suspect that money involved in this transaction is or represents proceeds of crime because the funds are coming from a country which I had never dealt with a transaction before." What the reporter, in fact, is trying to say is that "I do not know whether I should suspect that money involved in this transaction is or represents proceeds of crime, because I do not know whether such funds that comes from a country which I had never dealt with a transaction before corresponds to a money laundering method. Therefore, I am making a report out of caution." The UKFIU and Law Commission listed many examples where the reporting person accepts that they made a disclosure out of caution while they do not genuinely suspect that the funds are coming from criminal activity.[262] Thus, the problem is not that reporters do not understand what suspicion means. The problem is that some people subject to sections 327 to 329 of POCA 2002 do not have sources (eg. time, AML training etc.) to distinguish ordinary, unusual and suspicious transactions, and this inclines them to report all unusual transactions.

English law is unique among AML regimes, accepting the low threshold of suspicion for money laundering offences.[263] Sections 327 to 329 of POCA 2002 applies to everyone. An ordinary person who has no training on economic crimes, whether or not suspicion is defined, is improbable to successfully distinguish unusual and suspicious activities because they are highly unlikely to know what are money laundering methods and risk factors. Law-makers cannot expect everyone to be aware of criminal methods. Ponzi schemes are still finding many victims, showing that people are not aware of economic crime methods, and lawmakers cannot expect them to distinguish normal, unusual, and suspicious financial activities.[264]

The focus of this thesis is bankers' duty of reporting. Banks' directors, officers and employees constitute an informed group who can distinguish normal, unusual and suspicious activities.[265] AML laws require financial institutions to provide their staff with anti-money laundering training.[266] Moreover, the JMLG Guidance helps bankers distinguish expected, unusual and suspicious activities of banking clients by

[262] NCA's website, "SAR Quality Issues", available at: <https://www.ukciu.gov.uk/(b04b1m2pl1jooaqcnqutd3qe)/Information/info.aspx?InfoSection=Quality> 10 June 2021; and Law Commission (n.210), 97-98.
[263] Response of the Law Society of England and Wales to the consultation issued by the Home Office and HM Treasury on the Action Plan for anti-money laundering and counter-terrorist finance – legislative proposals (June 2016) in Law Commission (n.5), 14.4.
[264] K B Phelps and S Rhodes, *The Ponzi Book – A legal resource for unravelling ponzi schemes* (Matthew Bender Elite Products 2012), [1.04].
[265] See pages 158-159 in chapter 4.
[266] Regulations 24(1)(a)(ii) , and 24(2-3), The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

providing information relating to money laundering methods and risk factors.[267] Therefore, the "suspicion" term in sections 327 to 329 should not be seen as an excessively low threshold where such sections are applied to the banks and their staff.

Hence, following the ECtHR's decision in *Michaud v France*, this thesis defends that the notion of suspicions is a matter of common sense and that an informed group such as bankers can scarcely claim that they do not understand it in that the Court of Appeal gives specific guidance in *R v Da Silva*.[268]

Authorised disclosure. By making an authorised disclosure, the reporting person informs a competent person that he suspects that property is criminal property. Disclosure to a competent person by the alleged offender that property is criminal property may constitute an authorised disclosure in the following circumstances. First, a disclosure made before the alleged offender pursues the prohibited act constitutes an authorised disclosure.[269] If the alleged offender made a disclosure before he pursues the prohibited act, he must have the appropriate consent before pursuing the prohibited act.[270] Second, the alleged offender's disclosure while he is doing the prohibited act constitutes an authorised disclosure if he began to do the act at a time when, because he did not then know or suspect that the property constituted or represented a person's benefit from criminal conduct, the act was not a prohibited act, and the disclosure is made on his own initiative and as soon as is practicable after he first knows or suspects that the property constitutes or represents a person's benefit from criminal conduct constitutes an authorised disclosure.[271] Lastly, the alleged offender's disclosure after he pursued the prohibited act constitutes an authorised disclosure if he has a reasonable excuse for his failure to make the disclosure before he carried out the act, and he made the disclosure on his own initiative and as soon as it is practicable for him to make it.[272]

An authorised disclosure may be made to a nominated officer, a constable or a customs officer. 'Nominated officer' is a person nominated within a financial institution to submit SARs on behalf of the institution to the UKFIU.[273]

Prohibition of tipping off. One who acts within the regulated sector commits an offence under section 333A of POCA 2002 if he discloses to his client or a third party any information concerning an authorised or required disclosure which is likely to prejudice any investigation that might be conducted following the report. One who acts within the regulated sector commits tipping off offence if the

[267] The JMLG is a private sector body and therefore its' guidance cannot be legally binding. However, as it has HM Treasury approval, it is of importance for sections 330 and 331 of POCA 2002. Law Commission (n.5), [2.48].
[268] Michaud v France (2014) 59 E.H.R.R. 9, at [24].
[269] Section 338(2), POCA 2002.
[270] Sections 327(2), 328(2) and 329(2), POCA 2002.
[271] Section 338(2A), POCA 2002.
[272] Section 338(3), POCA 2002.
[273] Section 336, POCA 2002.

following two conditions are met: (1) the information on which the disclosure is based came to the alleged offender in the course of a business in the regulated sector, (2) the disclosure is likely to prejudice any investigation that might be conducted following the disclosure. The fact that the UK FIU gave consent to a transaction that is subject to an authorised report does not necessarily mean that an investigation will not be conducted in the future. The NCA clearly stated in its' guidance to reporters that "Appropriate consent signifies that either (a) action will not be taken by law enforcement agencies, (b) that law enforcement agencies do not require any further time in which to investigate or restrain assets or (c) a tactical decision has been taken to watch and wait."[274] It is worth noting that the legislator took measures in sections 333B to 333D of POCA 2002 not to inhibit information sharing required for the purposes of CDD and money laundering risk management within a financial group or between different institutions. A person guilty of a tipping off offence may be prosecuted with imprisonment for a term not exceeding two years or to a fine or to both .[275]

Appropriate consent. Tipping off rules are necessary but not sufficient for protecting the effectiveness of the SARs regime during the time of analysis undertaken by the person to which the disclosure is made. First, the reported transaction might be a transaction that would make tracing paper trail of criminal money impossible. Second, banking staff involved in criminal conspiracy may still inform criminals about the reports.[276] Therefore, one who made an authorised disclosure before pursuing the prohibited act should wait for the appropriate consent. The appropriate consent is the consent of the person to which the authorised disclosure is made, which may be a nominated officer, a constable or a customs officer. Providing a banking service to the client often amounts to a prohibited act. Therefore, the reported client's bank account should be frozen.

The client whose account is frozen may face significant financial hardship and loss of reputation. A barrister who had his both business and personal accounts frozen described the impact it had on him as follows:[277]

> … [I]t is simply inhumane to freeze a person's account for up to eight working days without giving him access to any money at all. (In my case I had £20 in cash in my flat and no food and there was no one in London who could help me. I was left absolutely desperate.)

In *Squirrell Ltd v National Westminster Bank plc*, a case that perfectly shows the impact of freezing accounts, the primary concern of Mr Khan, the managing director of Squirrel Ltd who had appeared on behalf of the company whose account was frozen following an SAR, was "to have the account unblocked so that the company can continue to make payments from it in the course of and for the purpose of maintaining its' business."[278] The financial hardship that the company faced was not limited

[274] Law Commission (n.5), [2.83]
[275] Section 333A, POCA 2002.
[276] See footnote 148 above.
[277] Law Commission (n,211), [5.110].
[278] *Squirrell Ltd v National Westminster Bank plc* [2005] 2 All ER 784, at [4].

to this. The notice by which Squirrell had launched the application before the court was drafted by Mr Khan. It was also Mr Khan who had appeared on behalf of the company both on the initial hearing of the application and on the full hearing. Mr Khan defended that "the reason for this [was] that [the reporting bank's] actions ha[d] deprived Squirrel of access to all readily available sources. The result [was] that it ha[d] not been able to pay lawyers to appear on its behalf".[279] Laddie J explained their views as follow[280]:

> I should say that I have some sympathy for parties in Squirrell's position…. Whatever one might feel, were Squirrell guilty of wrongdoing, if, as it says, it is innocent of any wrongdoing, this [the fact that while it is not proved or indeed alleged that the Squirrel Ltd or any of its associates has committed any offence, the company is faced to possible severe economic damage and is arguably deprived of the resources with which to pay lawyers to fight on its behalf] can be viewed as a grave injustice.

Prior to POCA 2002, the appropriate consent was given late by constables or customs officers in some cases.[281] Therefore, POCA 2002 introduced notice and moratorium periods. When the disclosure is made to a constable or a customs officer, the reporting person is treated as having the appropriate consent unless he receives, before the notice period expires, a notice which affirms that permission is refused.[282] The notice period is seven working days starting with the first working day after the disclosure.[283] One who filed an authorised report with a constable or a customs officer is treated to have the appropriate consent unless he receives a notice, before the moratorium period expires, which affirms that consent is refused.[284] Moratorium period is a period of 31 days, starting with the day on which the person receives notice that consent to the doing of the act is refused.[285]

A judge sitting at the Crown Court can extend the moratorium period for periods of up to 31 days.[286] The moratorium period can be extended by the Court up to 186 days in total after an application made by a senior officer.[287] Hence, moratorium period may go up to 217 days in total (31 days according to section 335 and 186 days according to section 336(A)). The Criminal Procedure Rules require notice to be served on the respondent[288], which includes, according to the definition of interested person made in section 336D(3), the reporting person as well as those who have an interest in the property that is subject

[279] Ibid, at [3].
[280] Ibid at [7].
[281] See section 93A to of the Criminal Justice Act 1988, where no time limits were incorporated and *Governor and Company of the Bank of Scotland v A Ltd* [2001] 1 WLR 751 and *Amalgamated Metal Trading Ltd v City of London Police Financial Investigation Unit* [2003] 1 WLR 2711.
[282] Section 335 (3), POCA 2002.
[283] Section 335 (3), POCA 2002.
[284] Section 335 (4), POCA 2002.
[285] Section 335 (6), POCA 2002.
[286] Section 336A (4), POCA 2002.
[287] Section 336A (2),(7), POCA 2002.
[288] Section 336B (7), POCA 2002 and Rule 47.64, Criminal Procedure rules.

of the disclosure (eg. the owner of the property or a third party such as an intended recipient of funds). Whilst, an interested person or anyone representing that person may be excluded by the court from any part of the hearing.[289] Moreover, after an application of the person who made the application for the extension of the moratorium period, the Court may decide for an order that specified information upon which the applicant intends to rely be withheld from an interested person and anyone representing that person.[290]

A banker who is not ready to take the risk of committing a money laundering offence cannot execute its customer's order during the notice or moratorium period unless consent was given by the person to which an authorised disclosure was made. The reporting person can neither honour the reported customer's mandate (see sections 327 to 329 and 335 of POCA 2002) nor offer an explanation for its inaction (see section 333A of POCA 2002) during the notice and moratorium periods. Laddie J, in *Squirrell Ltd v National Westminster Bank plc*, illustrated the way these provisions work by the facts of the case as follows:[291]

> Once NatWest suspected that Squirrell's account contained the proceeds of crime it was obliged to report that to the relevant authority, in this case the commissioners. It was also obliged not to carry out any transaction in relation to that account. That remains the position unless and until consent to the transactions is given by the commissioners or, if it is not, the relevant time limits under section 335 have expired. In the meantime, it is not allowed to make any disclosure to Squirrell which could affect any inquiries the commissioners might make. Obviously, telling Squirrell why it had blocked its account would constitute a prohibited disclosure.

Laddie J noted that she has some sympathy for parties in Squirrell's position, as "it is not proved or indeed alleged that it or any of its associates has committed any offence".[292] However, stressed out that ordering the bank to operate the account according to the client's instructions would require it to commit a criminal offence and that sympathy for the client's position does not override that consideration.[293]

The way the provisions mentioned above work may lead to problems between the reporting bank and the reported customer, particularly during the moratorium period. It is worth noting that of the 27,471 DAML SARs filed between October 2015 and March 2017, 12% resulted in deemed consent.[294] At the same period, "the average turnaround time for responses to reporters for all requests was between 5.8 and 6.2 days."[295]

---

[289] Section 336B(3), POCA 2002.
[290] Section 336B(4), POCA 2002.
[291] [2005] 2 All ER 784, at [19].
[292] [2005] 2 All ER 784, at [7].
[293] [2005] 2 All ER 784, at [21].
[294] Law Commission (n.5), 2.32.
[295] National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2017' 2017, 19.

2.IV.B.2.b. Bankers' right to make an authorised disclosure

The extent to which reporting person is protected from criminal and civil liability for acting in breach of any restriction on the disclosure of information is determined in section 338(4) of POCA 2002. In 2015, a new section, section 338(4A), was inserted by Serious Crime Act after section 338(4).

2.IV.B.2.b.i. Breach of any restriction on the disclosure of information: section 338(4) of POCA 2002

SARs produced by bankers may, and most of the time do, involve private, confidential and personal information.[296] Therefore, reporter interferes with the reported person's information privacy rights by making an authorised disclosure.

According to section 338(4) of POCA, "[a]n authorised disclosure is not to be taken to breach any restriction on the disclosure of information (however imposed)". By virtue of sections 327(2), 328(2), 329(2) and 340(3) of POCA 2002, one makes an authorised disclosure where he knows or suspects that funds constitute or represent proceeds of crime. Therefore, what suspicion means is essential to understand section 338(4).

Longmore LJ, in *K Ltd v NWB*, commented on the fact that there is no provision enabling the reporting banker to give evidence of his suspicion as follows: [297]

> This is not surprising. It may well have been the intention of the statute to protect those having a suspicion and reporting that suspicion to the authorities from being identified, since it is notorious that those concerned in money-laundering are no respecters of persons who report them to the authorities. This conclusion is bolstered by the further consideration that any cross-examination of a bank employee would, in fact, be almost as pointless as cross-examination of a bank's solicitor. Once the employee confirmed that he had a suspicion, any judge would be highly likely to find that he did indeed have that suspicion. Any cross-examination would be bound to decline into an argument whether what the employee thought could amount in law to a suspicion, which is not a proper matter for cross-examination at all.

His Lordship answered the counter-argument that "if this was the position, it would be all too easy for banks to assert a suspicion which was in fact groundless" as follows:[298]

[296] See pages 112-116.
[297] *K Ltd v NWB* [2006] EWCA Civ 1039 at [20].
[298] Ibid, [21]-[22].

> The answer … is twofold. (1) The existence of suspicion is a subjective fact. There is no legal requirement that there should be reasonable grounds for the suspicion. The relevant bank employee either suspects or he does not. If he does suspect, he must (either himself or through the bank's nominated officer) inform the authorities. (2) The provisions of the statute permitting only the bank's professional legal adviser to make a disclosure on its behalf, and then only for the purpose of court proceedings, cannot be sidestepped.
>
> The truth is that Parliament has struck a precise and workable balance of conflicting interests in the 2002 Act. It is, of course, true that to intervene between a banker and his customer in the performance of the contract of mandate is a serious interference with the free flow of trade. But Parliament has considered that a limited interference is to be tolerated in preference to allowing the undoubted evil of money-laundering to run rife in the commercial community. The fact that the interference lasts only for seven working days in what we were told were the majority of cases and a further 31 days only, unless the relevant authority goes to the length of applying to the court for a restraint order when all cards will have to be on the table in any event, shows that the interference with freedom of trade is limited. Many people would think that a reasonable balance has been struck.

Longmore LJ emphasised the difficulty of proving that one did not have a suspicion while discussing the reason why there is no provision enabling the reporting banker to give evidence of his suspicion.[299] This is by no means that one who confirmed that he had a suspicion is automatically accepted so. Indeed, in *Shah v HSBC*, the Court of Appeal held that the party who suffered loss as a result of SARs was entitled to demand proof from the regulated institution responsible that the suspicion on which the SAR was founded existed.[300] It is worth noting that, in *R v Da Silva*, the court held that "the essential element in the word "suspect" and its affiliates … is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist" [301].

2.IV.B.2.b.ii. Civil liability for damages: Section 338(4A) of POCA 2002

As explained above, if the alleged offender makes an authorised disclosure before he does the prohibited act, he must have the appropriate consent before doing the prohibited act.[302] The Court of Appeal in *K Ltd v National Westminster Bank plc*, put it that "if the law of the land makes it a criminal offence to

[299] Ibid, [20].
[300] *Shah v HSBC Private Bank (UK) Ltd* [2010] 3 All ER 477.
[301] *R v Da Silva* [2006] EWCA Crim 1654 at [16].
[302] Sections 327(2), 328(2) and 329(2), POCA 2002.

honour the customer's mandate in these circumstances there can .. be no breach of contract for the bank to refuse to honour its mandate".[303]

As explained above, the client whose account is frozen may face significant financial hardship and loss of reputation. Prior to 2015, only section in POCA 2002 that protects the reporting person was section 384. In 2015, section 338(4A) was inserted by Serious Crime Act after section 338(4). Section 338(4A) reads as follows: "Where an authorised disclosure is made in good faith, no civil liability arises in respect of the disclosure on the part of the person by or on whose behalf it is made." However, "there might be cases where an unwarranted disclosure (once proved to be so) could result in the affected party securing a remedy against a financial institution".[304]

2.IV.C. Required reports

Required reports under sections 330 and 331 of POCA 2002 differ from authorised reports in 3 respects. First, the duty and right to produce required reports apply to those who act within the regulated sector. Second, relevant persons are required and permitted to make a required report under three cumulative conditions: (1) the reporting person knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering; (2) the information came to the reporting person in the course of a business in the regulated sector and (3) the reporting person can identify the other person mentioned in the condition 1 or the whereabouts of any of the laundered property, or that he believes, or it is reasonable to expect him to believe, that the information or other matter mentioned in the condition 2 will or may assist in identifying that other person or the whereabouts of any of the laundered property. Third, one who made a required disclosure is not obliged to freeze the reported person's account.

2.IV.C.1. Required reports: Bankers' duty of reporting

One who fails to make a required disclosure in accordance with their obligations under Part 7 of POCA 2002 "may be liable for prosecution for one of three disclosure offences, depending on their status and whether they were acting within or outside the regulated sector".[305] Regulated sector is defined in Schedule 9 of the 2002 act. Businesses whose activity presents a high risk of money laundering, such

[303] *K Ltd v NWB* [2006] EWCA Civ 1039, at [10]. In relation to the implied terms related discussion, see *Shah v HSBC Private Bank (UK) Ltd* [2010] 3 All ER 477.
[304] Fortson QC (n.126), 173.
[305] Law Commission (n.5), [2.32]. See sections 330 – 332, POCA 2002.

as banks and credit institutions, are encompassed by the regulated sector.[306] A person guilty of an offence under sections 330 or 331 may be prosecuted with imprisonment for a term not exceeding five years or to a fine or to both[307].

Section 330 of POCA 2002 applies to any person working in the regulated sector, while section 331 applies to nominated officers only. 'Nominated officer' is a person nominated within a financial institution to submit SARs on behalf of the institution to the UKFIU.[308] One who is under duty to make a required report under section 330 of the act should file the report with a nominated officer, or a person authorised by the Director General of the National Crime Agency as soon as is practicable after the information comes to him.[309] If the report is sent to the nominated officer, the nominated officer, after investigating the issue, decides whether or not to file a report with the Financial Intelligence Unit. A nominated officer who is under duty to make a required disclosure under section 331 of the act should file the report with a person authorised by the Director General of the National Crime Agency as soon as is practicable after the information comes to him.

The reporting person is required to make a required disclosure under three conditions. "The first condition is that he knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering."[310] Not only one who knows or suspects but also one who has reasonable grounds for knowing or suspecting that another person is engaged in money laundering is under duty to make a required disclosure.

According to section 330(6) of POCA 2002, one does not commit an offence under section 330 if subsection 7 applies to him. Subsection 7 "applies to a person if (a)he does not know or suspect that another person is engaged in money laundering, and (b)he has not been provided by his employer with such training as is specified by the Secretary of State by order for the purposes of this section." Accordingly, one who does not know or suspect that another person is engaged in money laundering but has been provided by his employer with appropriate training can be prosecuted with an offence under section 330. Therefore, "reasonable grounds to suspect" is not a cumulative test. It is an objective test.[311] This means that it is sufficient for the prosecution to prove that, "objectively determined, a defendant had reasonable grounds for suspecting money laundering notwithstanding that he did not actually hold that suspicion"[312]. Lord Hughes in *R v Sally Lane and John Letts* put this as follows:[313]

---

[306] Law Commission (n.5), [2.33]. See section 1(1), Schedule 9 of POCA 2002.
[307] Section 334, POCA 2002.
[308] Section 336, POCA 2002.
[309] Sections 331 and 336, POCA 2002.
[310] Sections 330(2) and 331(2), POCA 2002.
[311] M Sutherland Williams, et all (n.171), [21.14].
[312] Law Commission (n.5), [8.39].
[313] *R. v Lane (Sally)* [2018] UKSC 36, at [22]. Similarly, see *R v Swan* [2011] EWCA Crim 2275; *R v Griffiths* [2006] EWCA Crim 2155; Also see M Goldby, 'Anti-money laundering reporting requirements imposed by English law: measuring effectiveness and gauging the need for reform' [2013] Journal of Business Law 367, 371; Law Commission (n.5), [8.37], [8.46].

> Section 21A (inserted into the Act by the Anti-terrorism, Crime and Security Act 2001) creates an offence, for those operating within the regulated sector, of non-disclosure of information suggesting an offence by another. By subsection (2) the first element of the definition of this offence is in the alternative:
>
> "The first condition is that he— (a) knows or suspects, or (b) has reasonable grounds for knowing or suspecting, that another person has committed or attempted to commit an offence under any of sections 15 to 18 ."
>
> In that section, or any other similarly constructed, it is plain beyond argument that the expression "has reasonable grounds for suspicion" cannot mean "actually suspects".

Taking into account subsections 6 and 7 of section 330, "it is plain beyond argument that the expression "has reasonable grounds for suspicion" cannot mean "actually suspects"".[314]

Goldby defends that the objective test in section 330 of POCA 2002 promotes over-caution and leads reporters to make defensive disclosures. She defends that the negligence test discourages the reporter from realistically evaluating the risk.[315] It is true that reporters make a significant number of defensive required disclosures. However, there are measures not to lead bankers to be over-cautious. First of all, there is the Joint Money Laundering Steering Group Guidance (the JMLG Guidance) which shows bankers what they should find suspicious.[316] Second, one does not commit an offence under section 330 of POCA 2002 if he does not know or suspect that another person is engaged in money laundering, and he has not been provided by his employer with such training as is specified by the Secretary of State.[317] Moreover, the second and third conditions in sections 330 and 331 of POCA 2002 may be seen as other measures against defensive reporting. Second condition listed in section 330 is that

> the information or other matter on which [the alleged offender's] knowledge or suspicion is based, or which gives reasonable grounds for such knowledge or suspicion, came to him in the course of a business in the regulated sector.[318]

A similar condition was put forward in section 331 too.[319] Third condition in sections 330 and 331 of POCA 2002 is related to the substance of the report. One may be under duty to make a required

---

[314] *R. v Lane (Sally)* [2018] UKSC 36, at [22]. Similarly, see *R v Swan* [2011] EWCA Crim 2275; *R v Griffiths* [2006] EWCA Crim 2155; Also see Goldby (n,313), 371; Law Commission (n.5), [8.37], [8.46].

[315] Goldby (n,313), 373.

[316] Sections 330(8) and 331(7) of POCA reads as follows

> In deciding whether a person committed an offence under this section the court must consider whether he followed any relevant guidance which was at the time concerned— (a)issued by a supervisory authority or any other appropriate body, (b)approved by the Treasury, and (c)published in a manner it approved as appropriate in its opinion to bring the guidance to the attention of persons likely to be affected by it.

The JMLG is a private sector body whose guidance has the HM Treasury approval. Therefore, it is of importance for sections 330 and 331 of POCA 2002. Law Commission (n.5), [2.48].

[317] Section 330(7), POCA 2002.

[318] Section 330(3), POCA 2002.

[319] Section 331(3), POCA 2002.

disclosure if he can identify the other person mentioned in the condition 1 or the whereabouts of any of the laundered property, or that he believes, or it is reasonable to expect him to believe, that the information or other matter mentioned in above mentioned condition 2 will or may assist in identifying that other person or the whereabouts of any of the laundered property.[320]

One does not commit an offence under sections 330 and 331 of POCA 2002, "if he has a reasonable excuse for not making the required disclosure".[321] Nor does a person commit an offence under these sections if

> (a)he knows, or believes on reasonable grounds, that the money laundering is occurring in a particular country or territory outside the United Kingdom, and
> (b)the money laundering—
> (i)is not unlawful under the criminal law applying in that country or territory, and
> (ii)is not of a description prescribed in an order made by the Secretary of State.[322]

Tipping off rules above-mentioned apply to those who made an authorised or required disclosure.

2.IV.C.2. Required reports: Bankers' right of reporting

SARs produced by bankers may, and most of the time do, involve private, confidential and personal information. Therefore, reporting person may interfere with the reported person's information privacy rights by making a required disclosure.

According to section 337 of POCA 2002, protected reports are "not to be taken to breach any restriction on the disclosure of information (however imposed)". A disclosure constitutes protected disclosure under three cumulative conditions: (1) "the information or other matter disclosed came to the person making the disclosure (the discloser) in the course of his trade, profession, business or employment", (2) "the information or other matter (a) causes the discloser to know or suspect, or (b) gives him reasonable grounds for knowing or suspecting, that another person is engaged in money laundering" and (3) the disclosure is made to a competent person "as soon as is practicable after the information or other matter comes to the discloser".[323]

From the perspective of the reporting banker, showing that he had suspicion is highly likely to be easier than showing that the information or other matter disclosed gave him reasonable grounds for suspecting, that another person is engaged in money laundering.[324] It is worth noting that a required report is highly

[320] Sections 330(5) and 331(3A), POCA 2002.
[321] Sections 331(5A) and 330(6), POCA 2002. Law Commission (n.5), [2.49].
[322] Sections 331(6A) and 330(7A), POCA 2002.
[323] Section 337, POCA 2002.
[324] 2.IV.B.2.b.i.

unlikely to cause financial loss to the reported person, because the reporting person is not under duty to automatically take further measures such as not honouring the client's orders.

2.IV.D. Conclusion

This part showed that English lawmakers gave effect to the FATF's STRs regime related recommendations by specifying low thresholds for a duty of reporting and serious punishment terms to apply those who fail to comply with their duty of reporting.

2.V. Swiss AML laws

2.V.A. Introduction

Banking industry has long had an important place in Swiss cantons' economy. Even in 14th century, people of Geneva were granted a right to lend money at interest by the Church.[325] More than 600 years after this unique privilege in Christendom, banking business still generates over 11% of gross domestic product in Swiss confederation.[326]

Financial concerns obliged Swiss cantons to establish a strong banking business, because they did not possess other means of production as they are situated in a mountainous and landlocked country.[327] Banks willing to attract clients from all over the world should accommodate their clients' needs, an important one of which is their need for financial privacy. Bank clients desperately need a financial centre where their privacy and secrecy is respected in times of international crisis, conflict or war. Switzerland is the first country whose perpetual neutrality was formally recognized by the international community.[328] Thanks to their political neutrality, Swiss cantons became a financial safe harbour in times of crisis, conflict or war.[329] In order to strengthen their financial safe haven status, Swiss cantons adopted strong bank secrecy laws. Laws of commerce laid down by the Great Council of Geneva in 1713, which is accepted as the first act in Europe that imposed upon banks a duty of secrecy, was elaborated in circumstances of war.[330] Currently, bankers' duty of secrecy in Swiss law differs from

[325] N Faith and A Macleod, 'The mysterious private banks of Geneva, Euromoney, <https://www.euromoney.com/article/b1d06hwcxgbq9y/the-mysterious-private-banks-of-geneva> 10 June 2021.
[326] R U Vogler, 'History' in Swiss Bankers Association's website. An extract taken from the "100 years of Swiss Banking. 100 people. 100 thank you", published for the 100th birthday of the SBA. <https://www.swissbanking.org/en/bankers-association/about-us/history> 10 June 2021.
[327] S Guex , 'The Origins of the Swiss Banking Secrecy Law and Its Repercussions for Swiss Federal Policy' (2000) 74 *Business History Review* 242.
[328] The perpetual neutrality of Switzerland was formally recognized by the international community within the Treaty of Paris (20 November 1815). See E F Malaspina, "History of International Law" in M Thommen *Introduction to Swiss law – Volume II* (Carl Grossmann Publishers 2018), 63. Some authors goes further defending that Switzerland's political neutrality dates back to the peace treaty the Swiss Confederacy signed with France on November 12, 1516. Eg. G E Sherman, 'The Neutrality of Switzerland' (1918) 12(2) The American Journal of International Law 241, 241.
[329] Faith and Macleod (n.325).
[330] Protestants who escaped from France transferred their wealth to Geneva, and Geneva bankers, known as French King's bankers, used Protestants' wealth to finance French monarch. One of the leading aims of 1713 bank secrecy

other professionals' duty of secrecy (eg. legal and medical professionals' duty of confidentiality), in being the only professional duty of secrecy whose breach is set forth as a criminal offence. Hence, economic reasons forced and political reasons enabled Switzerland to be 'the grandfather of financial secrecy'.[331]

Strong secrecy laws enabled bankers in neutral Swiss cantons to play an important role on behalf of investors and lenders in times of international crisis, conflict or war. There are three recent examples where Switzerland was a magnet for foreign investors who seek secrecy. First, in the 1920s, German citizens, who wished to avoid paying high taxes, invested in Switzerland where their secrecy was guaranteed with the bearer savings books practice[332]. At the time, Swiss bank secrecy rules caused conflict between Swiss authorities and France, willing to ensure that the German government collect a sufficient amount of tax to pay World War 1 debts.[333] Second, in the 1930s, German citizens with Jewish origin whose wealth was being chased by Nazis invested in Switzerland where their right to secrecy was protected by not only private law but also criminal law terms. Indeed, Article 47 of the Banking Act, where intentional or negligent breach of bank secrecy is set forth as a criminal offence, was adopted in 1934, shortly after the start of the holocaust. At the time, Swiss bank secrecy rules had been a subject of a conflict between Nazis and Swiss authorities.[334] Lastly, it is argued that the Nazis, after being defeated in World War II, invested in Switzerland where they had the chance to keep their identity secret[335].

As explained, financial reasons forced Switzerland, a small, landlocked and mountainous country, to develop an attractive financial sector. Switzerland, which is said to be the grandfather of financial secrecy,[336] adopted strong bank secrecy laws to create an attractive financial centre.[337] In 1994, same Switzerland established a voluntary SARs regime that applies to banks by adopting article 305ter

---

rules in the Great Council of Geneva was to protect secrecy of the fact that French King borrowed from 'protestant heretics'. Faith and Macleod (n.325); and M N Jovanović, *The Economics of International Integration* (Edward Elgar 2006), 395.

[331] Tax justice network, 'Narrative Report on Switzerland – financial secrecy index 2018', 2 <https://www.financialsecrecyindex.com/PDF/Switzerland.pdf> 10 June 2021. Banks' legal duty of secrecy was recognised in the regulations of the Great Council of Geneva more than 200 years before English courts recognised banks' legal duty of confidentiality. See The Great Council of Geneva 1713 regulations on banking registers. See also Jovanović (330), 395.

[332] Guex (n.327), 245.

[333] Ibid.

[334] For a detailed discussion of this issue, see *Ibid.*

[335] Vogler (n.326).

[336] Tax justice network (n.331), 2.

[337] See FATF (2016) (n.90), 19. Switzerland is not the only geographically and demographically small country who is famous with its' secrecy laws that has an attractive financial sector. See Tax justice network, 'Narrative Report on the Cayman Islands – financial secrecy index 2020' 1,2 <https://fsi.taxjustice.net/PDF/CaymanIslands.pdf> 10 June 2021; Tax justice network, 'Narrative Report on Luxembourg – financial secrecy index 2020, 2 <https://fsi.taxjustice.net/PDF/Luxembourg.pdf> 10 June 2021; Tax justice network, 'Narrative Report on Cyprus – financial secrecy index 2020, 1 <https://fsi.taxjustice.net/PDF/Cyprus.pdf> 10 June 2021. in relation to Cayman Islands, Luxembourg and Cyprus respectively.

paragraph 2 of SCC 1937, which entered into force on 1 august 1994. Accordingly, financial institutions were permitted but not obliged to report their money-laundering suspicions with law enforcement agencies.[338] However, the voluntary reporting system was not successful in persuading banks to make SARs. Therefore, AMLA 1997, which entered into force on 1 April 1998, established a mandatory reporting regime.[339] The Money Laundering Reporting Office (MROS) underlined that financial institutions produced around 30-40 SARs in 44 months from 1 August 1994 to 1 April 1998.[340] The MROS defended that the introduction of the duty to report paid off by increasing the number of SARs filed by financial institutions.[341] Indeed, financial institutions produced over 30 times more SARs in the next 44 months following the introduction of the duty to report.[342]

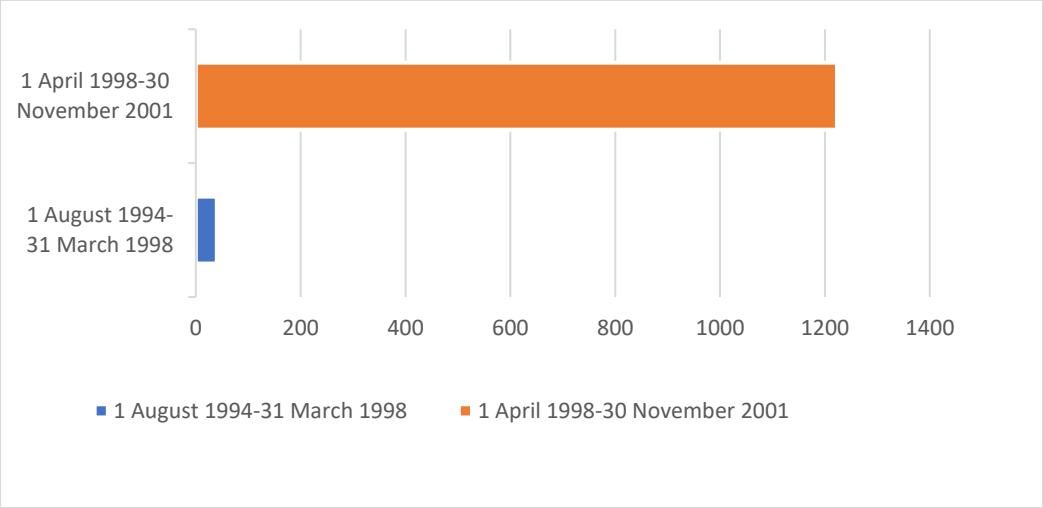


Chart 5: The number of SARs filed by financial institutions in Switzerland[343]

[338] See articles 305bis and 305ter of SCC 1937.
[339] Article 9, AMLA 1997.
[340] Office fédéral de la police, «Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 1998/1999», July 1999, 2.
[341] Ibid.
[342] According to the MROS's annual reports 1998, 1999, 2000 and 2001 financial institutions filed 1223 SARs in 44 months from 1 April 1998 to 30 November 2001. See Office fédéral de la police, *Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 1998/1999,* (July 1999), 35; Office fédéral de la police, «Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 1999/2000» June 2020, 25; Office fédéral de la police, «Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2000» July 2001, 10; Office fédéral de la police, «Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2001» May 2002, 9.
[343] This chart was created by using information provided in the MROS's 1998, 1999, 2000 and 2001 annual reports. See footnote 342.

2.V.B. The offence of money laundering

Swiss legislator criminalised money laundering in 1990 by adopting article 305*bis* of SCC 1937. The FATF's recommendation 3 advises countries to punish two types of attack on the dispositional interest in the value of rights, only the first one of which is accepted as a money laundering offence in Swiss law. One commits a money laundering offence according to article 305*bis* if he makes an act that aims to frustrate effective application of confiscation rules on the assets he knows or must assume is or represents criminal property. Swiss law is assessed 'largely compliant' with the requirements of the FATF's recommendation 3.[344]

2.V.B.1. *Prohibited act.*

According to article 305*bis* of SCC 1937, one commits a money laundering offence if he "carries out an act that is aimed at frustrating the identification of the origin, the tracing or the forfeiture of assets which he knows or must assume originate from a felony or aggravated tax misdemeanour".[345] Moreover, attempt to the offence of money laundering[346] as well as any form of participation to the offence of money laundering is punished.[347]

Paragraph 1 of article 305bis of SCC 1937 is translated to English in the Federal Council's website as follows:

> Any person who carries out *an act that is aimed at* [emphasis added] frustrating the identification of the origin, the tracing or the forfeiture of assets which he knows or must assume originate from a felony or aggravated tax misdemeanour is liable to a custodial sentence not exceeding three years or to a monetary penalty.

'[U]n act propre' and 'Handlung, die geeignet ist' expressions in original French and German texts of Article 305*bis* of SCC 1937 might have been translated as 'an act that is suited to'. Yet, this would have been in contradiction with the Federal Supreme Court's jurisprudence. An act that is not accepted as a prohibited act in one case may be accepted as a prohibited act in another case where the act is part of a

[344] FATF (2016) (n.90), 160; and FATF (2020), Anti-money laundering and counter-terrorist financing measures - Switzerland, Enhanced Follow-up Report & 2nd Technical Compliance Re-Rating, FATF, Paris, 11 <http://www.fatf-gafi.org/publications/mutualevaluations/documents/fur-switzerland-2020.html>.
[345] The Federal Council's website, Unofficial translation of Swiss Criminal Code of 21 December 1937, <https://www.admin.ch/opc/en/classified-compilation/19370083/index.html> 20 January 2020.
[346] ATF 120 IV 323 ss, 329/*JdT* 1996 IV 189, SJ 1995 308; TF, 8 decembre 2011, 6B_729/2010, cons. 4.4.2; ATF 138 IV 1/*JdT* 2013 IV 69.
[347] TF, 16 mars 2012, 6B_682/2011, cons. 3.1.

larger money-laundering scheme.[348] The issue is not whether the act is 'an act that is suited to' frustrating the identification of the origin, the tracing or the forfeiture of assets, it is whether the act is 'an act that is aimed at' it. According to the Federal Supreme Court's jurisprudence, the mere acceptance of funds[349], the mere depositing cash on a bank account[350] or the passive holding or custody of funds[351] do not in itself amount to money laundering provided the paper trail can be traced. However, these and a wide range of other acts constitute prohibited acts where they are part of a larger money-laundering scheme (eg. opening a bank account,[352] letting someone use your bank account to enable him to deposit or transfer money,[353] transferring money with banking transactions,[354] transporting money to another country by car,[355] hiding criminal money in an apartment[356]). It is worth noting that the offence of money laundering can also be committed by omission as far as the omission is "aimed at frustrating the identification of the origin, the tracing or the forfeiture of assets which .. [the alleged offender] knows or must assume originate from a felony or aggravated tax misdemeanour".[357] Indeed, the Federal Supreme Court established in 2010 that a financial intermediary may, as part of his role of guarantor, be guilty of money laundering by failing to produce a suspicious activity report in case where he knows or must assume that one of its' client's assets originate from a felony or aggravated tax misdemeanour.[358] Hence, one's failure to act in compliance with its' AML duties may amount to money laundering by omission as far as the alleged offender is under such legal duty and knows or must assume that the assets originate from a felony or aggravated tax misdemeanour. To conclude, the expression 'un acte propre à' has correctly been translated as 'an act that is aimed at'.

As explained above, a prohibited act for the purposes of the offence of money laundering is "an act that is aimed at frustrating the identification of the origin, the tracing or the forfeiture of assets" that can be subject to forfeiture terms [359]. Therefore, article 305bis "satisfies the requirements of Article 3(1)(b) of the Vienna Convention and Article 6(1)(a) of the Palermo Convention, in that it covers the acts of conversion, transfer, concealment and disguise",[360] while it does not "fully cover the acquisition,

[348] B Corboz, *Les infractions en droit suisse*, (Berne, Volume II, 2010), 637; T Hartsch, "Switzerland", in M Simpson, N Smith and A Srivastava (eds) *International guide to money laundering law and practice* (3rd ed, Bloomsbury Professional 2010) 1001.
[349] ATF 124 IV 274, ATF 127 IV 20.
[350] *ATF* 124 IV 274.
[351] BGer 6S. 595/1999 of 24 January 2000, and ATF 127 IV 20
[352] ATF 120 IV 323.
[353] TF, 20 Avril 2009, 6B_835/2008; TF, 12 decembre 2008, 6B_406/2008.
[354] TF, 5 mai 2003, 6S.35/2003, cons. 2.1; TF, 8 septembre 2003, 6S.22/2003, *ATF* 129 IV 322 ss, cons. 1.2.4, *SJ* 2004 I 115 ss.
[355] *ATF* 127 IV 20.
[356] TF, 14 aout 2002, 6S.702/2000 and 20 mai 2009, 6B_1021/2008. For further case law examples, see C Lombardini, *Banques et blanchiment d'argent* (3rd éd, Schulthess 2016), 86-92.
[357] O Abo Youssef and L Ruckstuhl "Switzerland" in *The international comparative legal guide to Anti-money laundering 2018* (Global Legal Group, 2018), [1.10] < https://iclg.com/practice-areas/anti-money-laundering-laws-and-regulations/switzerland> 20 January 2019.
[358] ATF 136 IV 188. FATF (2016) (n.90), 158; Lombardini (n.356), 90.
[359] Article 305*bis* of SCC 1937
[360] FATF (2016) (n.90), 158.

possession or use of the proceeds of a crime consistent with Article 3(1)(c)(i) of the Vienna Convention and Article 6(1)(b)(i) of the Palermo Convention."[361]

Swiss courts are empowered to prosecute an offence, including the offence of money laundering if the prohibited act took place in Switzerland.[362] It is worth mentioning that Swiss courts are competent if the criminal assets passed through the Swiss financial system even if the offender/(s) have never been in Switzerland.[363] Similarly, Swiss courts are competent if a company established in Switzerland has been used for the offence.[364]

2.V.B.2. Criminal property.

What is prohibited by article 305bis of SCC 1937 is "an act that is aimed at frustrating the identification of the origin, the tracing or the forfeiture of assets which he knows or must assume originate from a felony or aggravated tax misdemeanour". One's direct or indirect benefit from a felony or aggravated tax misdemeanour or any asset which represents such benefit constitutes criminal property if the alleged offender knows or must assume that it constitutes or represents such benefit.[365]

2.V.B.2.a. Condition – 1: One's direct or indirect benefit from a felony or aggravated tax misdemeanour or any asset which represents such benefit

Article 305bis of SCC 1937 criminalised frustrating the identification of the origin and the tracing of assets, because it aims to deter offenders from frustrating the forfeiture of illicit money.[366] According to the Federal Supreme Court's jurisprudence, 'frustrating the identification of the origin and the tracing of assets' conditions shall not have any independent significance in comparison to "frustrating the forfeiture'.[367] Therefore, 'assets' in article 305bis must be assets that can be subject to forfeiture terms.[368]

[361] FATF (2016) (n.90), 158.
[362] See articles 3 to 7 of SCC. See also, Lombardini (n.356), 75.
[363] TF, 27 septembre 2013, 1B_213/2013.
[364] TF, 2 decembre 2013, BB.2013.146, cons. 3.
[365] Judgement 6B 313/2008, 25 June 2008; ATF 120 IV 365, 19 December 1994; Judgement 1B 421/2011, 22 December 2011; TF, 28 decembre 2006, 6S.426/2006, *SJ* 2007 I 271 ss. See also FATF (2016) (n.90), 71-72.
[366] Lombardini (n.356), 87.
[367] TF, 4 avril 2003, 6S.226/2002, cons. 3.3, *ATF* 129 IV 238 ss/*JdT* 2007 IV 87 ss. See also Lombardini (n.356), 87; and Hartsch (n.348), 1002.
[368] Lombardini (n.356), 87.

Any asset obtained directly or indirectly by means of criminal activity may be subject to forfeiture terms,[369] as far as the prosecuting authority can prove all objective and subjective elements of the underlying offence[370] as well as the paper trail of the criminal property[371]. The court shall order the forfeiture of assets (i) that have been acquired through the commission of an offence,[372] (ii) that are intended to be used in the commission of an offence or as payment therefor,[373] or (iii) that are subject to the power of disposal of a criminal organisation.[374] The concept of offence covers both felonies (ie. offences that carry a custodial sentence of more than three years[375]), and misdemeanours (ie. offences that carry a custodial sentence not exceeding three years or a monetary penalty[376]).

While the title of article 305bis of SCC 1937 is 'money laundering', the notion of 'assets' includes all types of property.[377]

Some assets that can be subject to forfeiture terms cannot be considered as criminal property for the purposes of article 305bis. Article 305*bis* of SCC 1937 recognises only felonies and aggravated tax misdemeanour as predicate crimes for the offence of money laundering. Felony is any criminal offence that is punished with a prison sentence of more than three years.[378] According to paragraph 1bis of Article 305*bis* SCC 1937, a tax offence constitutes an aggravated tax misdemeanour under three conditions: (i) it must constitute a tax fraud (which implies the use of forged documents),[379] (ii) it must be in relation to direct taxes such as income tax,[380] and (iii) the tax evaded must exceed CHF 300,000 within a given tax period.[381]

Punishment of the money launderer does not depend on the punishment of the author of the predicate offence. As far as the Court is convinced that the predicate offence has been committed (all the elements

[369] Ibid,130.
[370] TF, 8 fevrier 2006, 6P.117/2005, cons. 2.3 and TF, 8 fevrier 2006, 6S.265/2005, cons 4.3.2; Cour de cassation, Geneve, 22 novembre 1996, *SJ* 1997 186 ss.
[371] TF, 26 mai 2003, 6S.709/2000 and 6S.710/2000, cons. 6.3; TF, 14 novembre 2007, 6B_369/2007; TF, 24 mars 2013, 1B_711/2012.
[372] Article 70, SCC 1937.
[373] Article 70, SCC 1937.
[374] Article 72, SCC 1937..
[375] Article 10(2), SCC 1937.
[376] Article 10(3), SCC 1937.
[377] Lombardini (n.356), 72.
[378] Article 10 (2), SCC 1937. Some examples of felony: Theft in article 139, Robbery in article 140, Fraud in article 146, Computer fraud in article 147 and Misuse of a cheque card or credit card in article 148 of SCC 1937, drug dealing (article 19(2) of the Federal Act on Narcotics and Psychotropic Substances), bribery (article 322-ter SCC 1937) and participation in a criminal organisation (article 260-ter SCC 1937).
[379] See Article 186 of the Federal Act of 14 December 1993 on Direct Federal Taxation and Article 59 paragraph 1 clause one of the Federal Act of 14 December 1994 on the Harmonisation of Direct Federal Taxation at Cantonal and Communal Levels. See TF, 17 aout 2015, 6B_408/2015.
[380] For indirect taxes, see article 14(4) of Loi federal sur le droit penal administratif du 22 mars 1974, RS 313.0.
[381] For further details, see Lombardini (n.356), 77-85.

of the predicate offence were met and there is no defence applicable), there is no requirement that a person be convicted of a predicate offence to prove that property is the proceeds of crime.[382]

As underlined in the FATF's 2016 Mutual Evaluation Report, Swiss financial system is attractive for assets derived from offences that are committed abroad.[383] As opposed to its' English counter-part, Swiss AML law applies a dual criminality test for predicate offences committed abroad. Accordingly, one may be liable with a money laundering offence even if the predicate offence was committed abroad as long as this offence is punishable both in Switzerland and in the relevant country.[384]

2.V.B.2.b. Condition – 2: One who knows or must assume

One's benefit (property or pecuniary advantage)[385] from a felony or aggravated tax misdemeanour or any asset which represents such benefit constitutes criminal property[386] if the alleged offender knows or must assume that it constitutes or represents such benefit. Because not only those who know that the assets originate from a felony or aggravated tax misdemeanour but also those who must assume that the assets originate from a felony or aggravated tax misdemeanour can be liable for a money laundering offence, knowledge of the criminal origin of the laundered property may be inferred from objective factual circumstances.[387] Objective circumstances cover a long list of factors such as the nature of the relation between the alleged money launderer and the economic criminal for whom criminal money is laundered[388] and the nature of the prohibited act.[389]

The *mens rea* of money laundering is recklessness (*dol eventuel*). The Federal Supreme Court established that "this element is already met when the perpetrator considers the harmful outcome as possible, but acts nevertheless because he/she accepts the possibility of the outcome and resigns to it, even if he/she deems it undesirable and does not wish it".[390]

---

[382] ATF 138 IV 1 ss/*JdT* 2013 IV 69 ss; TF, 12 aout 2008, 6B_482/2007; TF, 26 Avril 2011, 6B_91/2011; FATF (2016) (n.90), 159; Lombardini (n.356), 74.
[383] FATF (2016) (n.90), 3 and 5 (referring to Swiss National Risk Assessment report published in June 2015).
[384] SCC 1937, Article 305*bis1* (3). For further details, see TF, 27 septembre 2013, 1B_213/2013; TPF, 2 decembre 2013, BB.2013.146, cons. 3; and Lombardini (n.356), 76-77.
[385] Article 305bis(1bis) of SCC 1937. See Lombardini (n.356), 90-91.
[386] Judgement 6B 313/2008, 25 June 2008; Federal Supreme Court, ATF 120 IV 365, 19 December 1994; Judgement 1B 421/2011, 22 December 2011; TF, 28 decembre 2006, 6S.426/2006, *SJ* 2007 I 271 ss. See also FATF (2016) (n.90), 159 and Lombardini (n.356), 71-72.
[387] TF, 25 juin 2007, 6P.49/2007, cons 9.3. See also FATF (2016) (n.90), 159 , 3.8. and Lombardini (n.356), 93 and Hartsch (n.348), 1003.
[388] ATF 138 IV 1/*JdT* 2013 IV 69; TF, 21 octobre 2010, 6B_900/2009, cons. 6.2.2, *ATF* 136 IV 179/*JdT* 2011 IV 143, *SJ* 2011 I 21. TF, 20 avril 2009, 6B_835/2008, TF, 18 juillet 2013, 6B_627/2012.
[389] TF, 18 juillet 2013, 6B_627/2012.
[390] TF, 23 mars 2001, 6S.778/2000, cons, 2 c aa, as translated in FATF (2016) (n.90), 159.

2.V.B.3. Sanctions

Compared to its' English counter-part, the Swiss Criminal Code specified relatively mild sanctions.[391] According to Article 305*bis1* of SCC 1937, the offence of money laundering is to be prosecuted with "a custodial sentence not exceeding three years or to a monetary penalty". In serious cases, however, money launderers may be convicted to "a custodial sentence not exceeding five years or a monetary penalty (a custodial sentence is combined with a monetary penalty not exceeding 500 daily penalty units)". There is not an exhaustive list of serious cases. A serious case may be found, in particular, where the offender acts as a member of a criminal organisation, acts as a member of a group that has been formed for the purpose of the continued conduct of money laundering activities or achieves a large turnover or substantial profit through commercial money laundering[392].

Both real and legal persons can independently and primarily be penalised for the offence of money laundering.[393] Money laundering is a failure to prevent model offence for undertakings. Indeed, according to article 102 of SCC 1937:

> "If a felony or misdemeanour is committed in an undertaking in the exercise of commercial activities in accordance with the objects of the undertaking and if it is not possible to attribute this act to any specific natural person due to the inadequate organisation of the undertaking, then the felony or misdemeanour is attributed to the undertaking. In such cases, the undertaking is liable to a fine not exceeding 5 million francs.
>
> If the offence committed falls under Articles […] 305*bis [money laundering]* […], the undertaking is penalised irrespective of the criminal liability of any natural persons, provided the undertaking has failed to take all the reasonable organisational measures that are required in order to prevent such an offence".

Therefore, a legal person can independently and primarily be liable for a money laundering offence if the prosecution can prove that the offence is related to the corporate purpose[394] and that "the undertaking has failed to take all the reasonable organisational measures that are required in order to prevent such an offence"[395].

The perpetrator of the predicate offence may be sentenced for a money laundering offence in Switzerland[396]. As opposed to sections 327 and 329 of POCA, the ambit of article 305bis of SCC is

---

[391] Preller, (n.211), 237.
[392] SCC 1937, Article 305*bis1* (2). Eg. TF, 5 mai 2003, 6S.35/2003, cons 2.3; and TF, 22 septembre 2003, 6S.272/2003.
[393] Hartsch (n.348), 1001.
[394] D Poncet, A Macalusa, «Evolution de la responsabilité pénale de l'entreprise en Suisse et perspective inspirée de modèles étrangères», in *Strafrecht, Strafprozessrecht und Menschenrechte, Fetschrift fur Stefan Trechsel*, (Zurich 2002) 518-521; and Hartsch (n.348), 1001.
[395] Article 102 of SCC 1937
[396] Article 305bis of SCC. See *ATF* 120 IV 323 ss/*JdT* 1996 IV 189, SJ 1995 308; *ATF* 122 IV 211 ss/*JdT* 1997 IV 165 ss; *ATF* 124 IV 274 ss/*JdT* 1999 IV 81 ss, *SJ* 1991 I 193 ss; *ATF* 126 IV 255.

narrow. One commits a money laundering offence under article 305bis if he makes an act that is aimed at frustrating the identification of the origin, the tracing or the forfeiture of criminal assets. Therefore, one who committed an economic crime and benefited from the proceeds of his crime is not automatically liable for a money laundering offence.

2.V.C. Permitted reports

Swiss legislator criminalised money laundering in 1990 by adopting article 305*bis* of SCC 1937. Article 305*bis*, as adopted in 1990, prescribed that one who carries out an act that is aimed at frustrating the identification of the origin, the tracing or the forfeiture of assets which he knows or must assume originate from a felony commits a money laundering offence. Accordingly, banks and their staff were responsible for a money laundering offence where they provided service to their clients on assets they know or must assume originate from a felony.

Swiss law did not regulate bankers' right to make an SAR until 1994. Therefore, bankers faced a dilemma from August 1990 to March 1994, where money laundering was recognised as a criminal offence yet a voluntary or mandatory SARs regime was not yet developed. A banker who suspects that their client's funds are proceeds of crime has three options: (i) keep providing service to the client, (ii) terminating the business relationship with the client and restoring the suspicious funds, and (iii) sharing the suspicion with the law enforcement agencies.

First, a banker who suspects that their client's funds are proceeds of crime yet keeps providing service to the client takes the risk of being prosecuted with a money laundering offence. The bankers were worried about the possibility that the court can assess that the banker was in a position in which he must have assumed that their client's assets originated from a felony. [397] Second, where the banker puts an end to their business relationship with their client due to their doubts and restores the suspicious funds, the banker again takes the risk of being prosecuted with a money laundering offence.[398] This is because restoring the funds may amount to a prohibited act. Moreover, terminating the business relation on the basis of mere suspicion may give rise to financial loss and damage to the reputation of the financial institution. This may affect the attractiveness of the financial institution. Third, a banker who wished to inform the prosecution authorities of his situation was taking the risk of violating their duty of secrecy.[399] It is worth noting that intentional or negligent breach of bank secrecy was set forth as a criminal offence in Switzerland.[400]

[397] «Message concernant la modification du code pénal suisse et du code pénal militaire» FF 1993 III 269 , 314.
[398] FF 1993 III 269 (n.397), 314.
[399] Ibid.
[400] Article 47 of Swiss Federal Act on Banks and Savings Banks 1934.

Swiss legislator introduced paragraph 2 of article 305*ter* of SCC 1937 to solve above-explained problem.[401] Paragraph 2 of article 305ter as enacted in 1994 prescribed that

> The persons included in paragraph 1 above *[any person who as part of his profession accepts, holds on deposit, or assists in investing or transferring outside assets]* are entitled to report to Swiss prosecution authorities indications that establish suspicion that assets originate from a felony.[402]

In 1997, AMLA 1997 was adopted. Article 11(2) reiterated that any person who filed a report under Article 305*ter* paragraph 2 SCC 1937 "may not be prosecuted for a breach of official, profession or trade secrecy or be held liable for breach of contract."[403]

In 1998, the Money Laundering Reporting Office Switzerland (MROS) in the Federal Office of Police was established as Switzerland's financial intelligence unit.[404] In 2014, aggravated tax misdemeanour was recognised as a predicate offence for the purposes of article 305bis of SCC 1947.[405] Accordingly, article 305ter paragraph 2 was changed as follows:

> The persons included in paragraph 1 above *[any person who as part of his profession accepts, holds on deposit, or assists in investing or transferring outside assets]* are entitled to report to the Money Laundering Reporting Office in the Federal Office of Police indications that establish suspicion that assets originate from a felony or an aggravated tax misdemeanour in terms of Article 305bis number 1bis.[406]

Article 305ter paragraph 2 was translated to English in the Federal Council's website as follows:

> The persons included in paragraph 1 above are entitled to report to the Money Laundering Reporting Office in the Federal Office of Police any observations that indicate that assets originate from a felony or an aggravated tax misdemeanour in terms of Article 305bis number 1bis.

Federal Council's unofficial translation is mistaken by not referring at all to suspicion, while the original French text of the article referred to "les indices fondant le soupçon".

The reporting person is entitled to disclose "indications that establish suspicion that assets originate from a felony or an aggravated tax misdemeanour".[407] Hence, the reporting bank's observation should

---

[401] Lombardini (n.356), 147.
[402] FF 1993 III 269 (n.397), 269.
[403] Article 11(2), AMLA 1997. Unoffical translation of Federal Act of 10 October 1997 on Combating Money Laundering and Terrorist Financing in the Financial Sector in the Federal Council's website: <https://www.fedlex.admin.ch/eli/cc/1998/892_892_892/en> 10 June 2021.
[404] P Fischer et al, «Développements actuels en droit pénal, fiscal et réglementaire : impacts significatifs sur la profession d'avocats» (2015) *Revue de l'avocat* 418, 424.
[405] For further details, see «Loi fédérale sur la mise en œuvre des recommandations du Groupe d'action financière, révisées en 2012», RO 2015 1389 and C Balmat «Le GAFI en passe de criminaliser les délits fiscaux» *L'expert-comptable Suisse* 287, 289.
[406] Translated from its' original French by the author of this thesis.
[407] Article 305ter (2), SCC 1937.

amount to suspicion.[408] However, the MROS defended in its 2012 annual report and its website that "within the framework of Article 305*ter* paragraph 2 SCC, a financial intermediary can file a report based on a likelihood, a doubt or even a sense of unease about continuing the business relationship"[409]. Hence, MROS interpreted article 305ter in a way it excessively protects bankers from criminal and civil liability where they make a permitted disclosure. The MROS has not provided any explanation to justify its argument that "indications that establish suspicion" includes even a sense of unease. The MROS is an administrative authority and all acts of administrative authorities, must be "based on and limited by law".[410] MROS's relevant interpretation in its' annual report contradicts the text of the article and constitutional principles.[411] It is worth mentioning that mistaken English translation of Article 305ter of SCC 1937 on the Federal Council's website seems to be made in compliance with the MROS's interpretation. Indeed, federal council's website translated "les indices fondant le soupçon que des valeurs patrimoniales proviennent d'un crime ou d'un délit fiscal qualifié au sens de l'art. 305bis, ch. 1bis" as "any observations that indicate that assets originate from a felony or an aggravated tax misdemeanour in terms of Article 305bis number 1bis".

Making a permitted disclosure in compliance with article 305ter paragraph 2 of SCC 1937 is not recognised as an exemption or a general defence in article 305*bis*. One who carries out an act that is aimed at frustrating the identification of the origin, the tracing or the forfeiture of assets which he knows or must assume originate from a felony or aggravated tax misdemeanour is responsible for a money laundering offence regardless of whether or not he produced a suspicious activity report.[412] However, the fact that a suspicious activity report was produced by the alleged offender may affect the assessment of circumstances. Bacher defends that, whether or not a suspicious activity report was produced by the alleged offender and the content of the report, if there is any, should be taken into account in determining whether the alleged offender was in a situation where he must have assumed that the assets at stake originated from a felony or aggravated tax misdemeanour.[413] Lombardini defends that one who made

[408] See TF, 20 decembre 2013, BB.2013.115; *ATF* 128 IV 145 ss, *JdT* 2004 IV 32, *SJ* 2002 I 565; *ATF* 142 IV 333 Tribunal Federal's observations relating to suspicions word used in Article 9 of AMLA 1997. Office fédéral de la police, «Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2007» 2007, 86; FATF (2016) (n.90), 195.

[409] Office fédéral de la police, «Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2012» July 2012, 88; see also Federal Office of Police website, "Art. 305ter para. 2 SCC – right to report a mere suspicion" <https://www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/geldwaescherei/meldung/meldeformular/art_305_stgb.html> 10 June 2021.

[410] Article 5(1) of the Federal Constitution of the Swiss Confederation.

[411] Lombardini (n.356), 160.

[412] TPF, 20 mars 2007, SK.2006.19.

[413] J L Bacher, « Jurisprudence du TPF en matière de blanchiment d'argent: de gestion déloyale et d'escroquerie » (2011) *L'expert-comptable Suisse* 238, 245.

an SAR, required or permitted, should benefit from a presumption that he wanted to act in compliance with article 305bis SCC.[414]

2.V.D. Required reports

Swiss law-maker established a voluntary reporting regime in 1994. However, the voluntary reporting system was not used by financial institutions as much as expected. The Money Laundering Reporting Office (MROS) underlined that financial institutions produced around 30-40 SARs in 44 months from 1 August 1994 to 1 April 1998.[415] Therefore, the Swiss legislator established a mandatory reporting system in 1998.

In 1997, the Swiss legislator adopted AMLA 1997. Paragraph 1 of Article 9 (1) of AMLA 1997 was translated in the Federal Council's website as follows[416]:

> 1. A financial intermediary must immediately file a report with the Money Laundering Reporting Office Switzerland (the Reporting Office) as defined in Article 23 if it:
>
> a. knows or has reasonable grounds to suspect that assets involved in the business relationship:
>
> 1. are connected to an offence in terms of Article 260ter Number 1 or 305bis SCC,
>
> 2. are the proceeds of a felony or an aggravated tax misdemeanour under Article 305bis number 1bis SCC,
>
> 3. are subject to the power of disposal of a criminal organisation, or
>
> 4. serve the financing of terrorism (Art. 260^{quinquies} para. 1 SCC);
>
> b. terminates negotiations aimed at establishing a business relationship because of a reasonable suspicion as defined in letter a;
>
> c. knows or has reason to assume based on the clarifications carried out under Article 6 paragraph 2 letter d that the data passed on by FINMA, the FGB, a supervisory organisation or a self-regulatory organisation relating to a person or organisation corresponds to the data of a customer, a beneficial owner or an authorised signatory in a business relationship or transaction.

Paragraph 1(a)'s translation is mistaken. "[S]'il sait ou présume, sur la base de soupçons fondés, que…" should have been translated as "if it knows or assumes, based on well-founded suspicion, that…". In its' 2016 Mutual Evaluation report, the FATF officials also preferred the latter.[417] Mistranslation in

[414] Lombardini (n.356), 163; J B Zufferey, C Lombardini, « L'obligation subsidiaire d'annonce et de dénonciation des 'ORA LBA' » (2007) *AJP* 1096, 1099.
[415] Office fédéral (n, 340), 2.
[416] AMLA 1997's unoffical English translation available at the Federal Council's website: <https://www.fedlex.admin.ch/eli/cc/1998/892_892_892/en> 10 June 2021
[417] FATF (2016) (n.90), 194.

paragraph 1(a) affects the meaning of paragraph 1(b) too. Paragraph 1(b) should be understood as follows:[418]

> financial intermediary that terminates negotiations aimed at establishing a business relationship because it knows or assumes, based on a well-founded suspicion, that assets involved in the business relationship are connected to money laundering or participation or supporting a criminal organisation offences, are the proceeds of a felony or an aggravated tax misdemeanour, are subject to the power of disposal of a criminal organisation, or serve the financing of terrorism.

The Federal Council, in its 1996 report that introduced Anti Money Laundering Bill, defended that suspicion is deemed well-founded "where there are concrete signs or several indicia that suggest the origin of the assets is unlawful".[419] However, the courts and the MROS interpreted 'well-founded suspicion' more extensively. Accordingly, there is well-founded suspicion where there is a mere doubt as to the legal origin of asset.[420] Moreover, the Federal Supreme Court takes into account banking institutions' CDD duties in deciding whether there is well-founded suspicion.[421] Financial intermediaries are required to report any suspicions raised around a customer's activity as a whole, not necessarily based on a transaction.[422]

Swiss AMLA 1997, where financial institutions' duty of reporting is regulated, applies to "financial intermediaries" as well as "natural persons and legal entities that deal in goods commercially and in doing so accept cash (dealers)".[423] Financial intermediaries cover, among others, banks as defined in

[418] Lombardini (n.356), 153.
[419] « Message relatif à la loi fédérale concernant la lutte contre le blanchissage d'argent dans le secteur financier, 96.055 » FF 1996 III 1057, 1086.
[420] TF, 20 decembre 2013, BB.2013.115; *ATF* 128 IV 145 ss, *JdT* 2004 IV 32, *SJ* 2002 I 565; *ATF* 142 IV 333; Office fédéral de la police (n.408), 86; FATF (2016) (n.90), 195.
[421] ATF 136 IV 188, 3 November 2010. FATF (2016) (n.90), 158.
[422] *ATF* 128 IV 145 ss, *JdT* 2004 IV 32, *SJ* 2002 I 565; TPF, 20 decembre 2013, BB.2013.115; Office fédéral de la police (n.408), 88.
[423] Article 2(1), AMLA 1997.

articles 1a[424] and 1b[425] of the Swiss Federal Act on Banks and Saving Banks 1934.[426] All financial sector products and services of banks are subject to relevant AML/CTF regulations.[427]

According to article 37 of AMLA 1997:[428]

> Any person who fails to comply with the duty to report in terms of Article 9 shall be liable to a fine not exceeding 500,000 francs.
>
> If the offender acts through negligence, he or she shall be liable to a fine not exceeding 150,000 francs.

The offence of money laundering specified in article 305bis of SCC 1937 can be committed by action or omission. The Federal Supreme Court in 2010 decided that a financial intermediary may, as part of his role of guarantor, be guilty of money laundering by failing to produce a required report in case where it knows or must assume that one of its' clients' assets originate from a felony or aggravated tax misdemeanour.[429] Therefore, failure to produce a SAR by a financial intermediary may amount to money laundering by omission as far as the alleged offender knows or must assume that one of its' clients' assets originate from a felony or aggravated tax misdemeanour. An employee of the bank who is in charge of making required disclosure is also required to play a guarantor role by virtue of article 9 of AMLA 1997 and its' contractual duties. Therefore, banking staff who is under a duty to make required disclosure and who fails to do so may commit a money laundering offence. Lombardini and Conrad Hari criticised the Federal Supreme Court's decision arguing that it equalises the responsibility of financial intermediaries and their staff, on the one hand, and policemen, on the other hand.[430] However, it is worth noting that it is not the Federal Supreme Court that mistakenly gave financial intermediaries policeman duties, it is the legislator who intentionally gave such duties to the financial intermediaries by adopting AMLA 1997.[431]

---

[424] According to article 1a of the Swiss Federal Act on Banks and Saving Banks 1934, "A bank shall be an institution primarily active in the financial sector that (a) accepts deposits from the public in excess of CHF 100 million on a professional basis or that publicly advertises as doing so; (b) accepts deposits from the public up to CHF 100 million on a professional basis or that publicly advertises as doing so, and which invests or gives interest on the deposits received from the public; or (c) on a large scale refinances itself with loans from banks that do not own any significant holdings in it in order to finance for own account and in any manner possible any number of persons or companies with which it does not form an economic unit." 'Unofficial translation of the Swiss Federal Act on Banks and Savings Banks' (KPMG, 1 January 2016).

[425] Persons mentioned in article 1b of the Swiss Federal Act on Banks and Saving Banks 1934 are "persons that are primarily active in the financial sector, and: (a) accept deposits from the public up to CHF 100 million on a professional basis or who publicly advertise as doing so; and (b) which neither invest nor give interest on these deposits from the public." Unofficial translation (n.424).

[426] Article 2(2), AMLA 1997.

[427] Lombardini (n.356), 43.

[428] Unoffical English translation (n.416).

[429] ATF 136 IV 188. See also Abo Youssef and Ruckstuhl (n.357), [1.10]

[430] Lombardini (n.356), 90; A Conrad Hari, «Le blanchiment d'argent par omission» (2012) *RSDA* 361, 372.

[431] Corboz (n. 348), n° 23 ad art. 305bis CP.

Prior to 2016, there was an important difference between the immediate effect of the required and permitted reports. Once a financial intermediary filed a required report, it was immediately under a duty to freeze the relevant client's account for five working days unless the MROS informs the reporting person that such measure is not necessary.[432] However, the reporters were not under such duty when they filed a permitted report.

The number of SARs received by the MROS significantly increased between 2000 and 2015.[433] Therefore, the reporting person's duty to freeze the reported person's account was changed in 2016. In the last 5 years, the MROS reached a point where it is no more able to deal with all the reports it received. For instance, in 2019, the MROS managed to deal with only 52.9 % of the SARs received in the same year.[434]

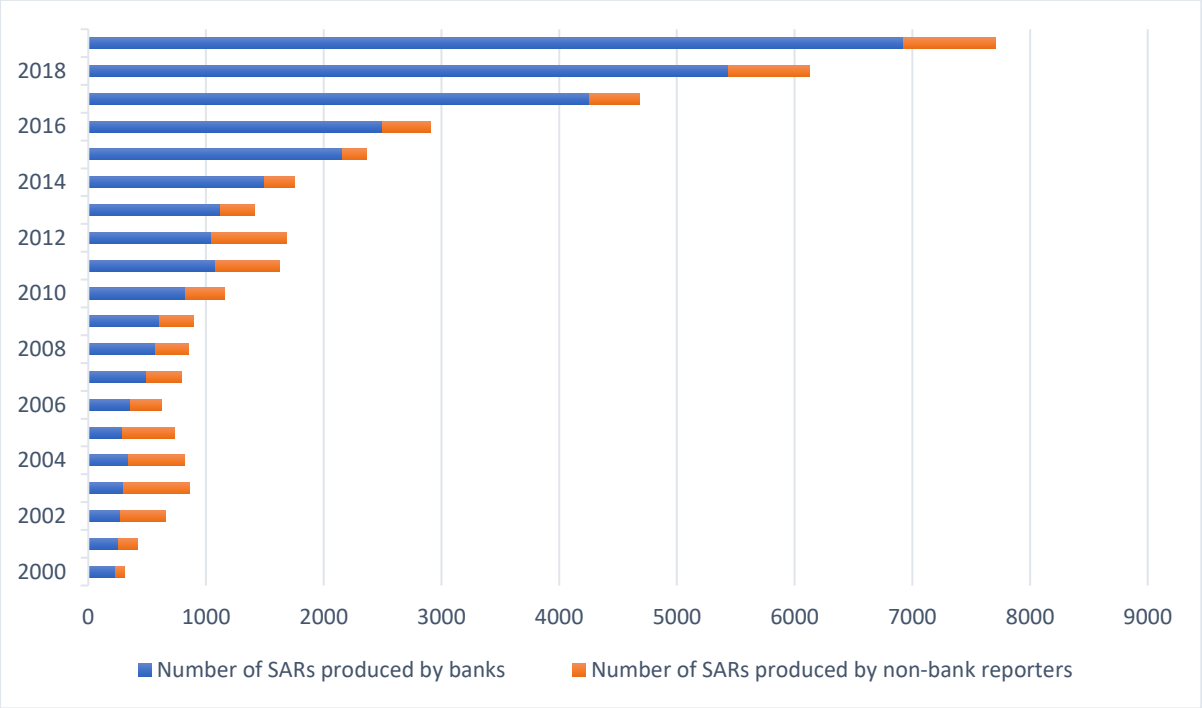


Chart 4: The number of SARs Swiss private sector produced per year[435]

[432] Article 10, AMLA 1997.
[433] MROS received 311 and 2367 SARs in the years 2000 and 2015 respectively. Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2015', (Avril 2016), 7.
[434] Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2019', (Avril 2020), 7;
[435] See Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2019', (Avril 2020), 7; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2018', (Avril 2019), 8; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2017', (Avril 2018), 8; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2016', (Avril 2017), 8; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2010', (Avril 2011), 9; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2005', (Avril 2016), 9.

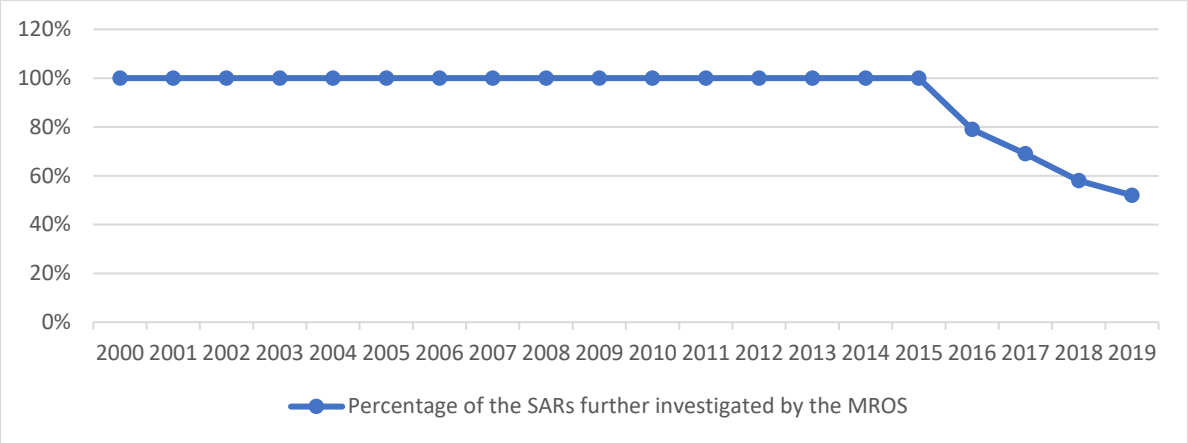


Chart 5: Percentage of the SARs further investigated by the MROS [436]

Currently, during the analysis conducted by the MROS of a required or permitted report, the financial intermediary shall execute customer orders relating to the assets reported under Article 9 -1(a) of AMLA 1997 or under Article 305*ter* (2) of SCC 1937.[437] According to Article 10 of AMLA, the financial intermediary shall freeze the assets entrusted to it that are related to the report (ie. a report filed under Article 9 -1 (a) of AMLA 1997 or under Article 305ter (2) of SCC 1937) as soon as the MROS informs it that the report has been forwarded to the prosecution authority. The financial intermediary shall continue to freeze the assets until it receives a ruling from the competent prosecution authority, but at most for five working days from the date on which the MROS gives notice of forwarding the report to the prosecution authority.[438]

SARs produced by bankers may, and most of the time do, involve private, confidential and personal information. Therefore, reporting person may interfere with the reported person's information privacy rights by making a disclosure. It is highly unlikely that a report filed under Article 9 -1 (a) of AMLA 1997 or under Article 305*ter* (2) of SCC 1937 causes financial loss to the reported person because the reporting person is not under a duty to freeze the client's account automatically.[439]

Prior to 1 February 2009, one who filed a report according to article 9 of AMLA 1997 was protected from criminal and civil liability for producing a report where he can demonstrate that he exercised the diligence required by the circumstances. Moreover, prior to 2016, the reporting bank was required to

[436] See footnote 435 above.
[437] Article 9a, AMLA 1997.
[438] Article 10, AMLA 1997.
[439] Lombardini (n.356), 161.

freeze the reported person's account for 5 working days unless the MROS informs the reporting person that such measure is not necessary. Therefore, the reporting bank was responsible for damages of the client about whom a required report was filed unless the bank can prove that it exercised the diligence required by the circumstances.

Currently, article 11 of AMLA 1997 reads as follows:

> Any person who in good faith files a report under Article 9 of this Act or who freezes assets in accordance with Article 10 may not be prosecuted for a breach of official, profession or trade secrecy or be held liable for breach of contract.

Hence, banks and their staff who in good faith files a report under Article 9 or who freeze its' client's account in accordance with Article 10 are protected from criminal and civil liability. Acting in good faith is explained in article 2(1) of Code civil, and means acting honestly and respectful to others' rights.[440] Hence, bank and its staff are protected from criminal and civil liability where they can show that they had a pertinent reason that justifies their filing the report.[441] Acting in good faith is a lower threshold compared to demonstrating the exercise of the diligence required by the circumstances.[442] Compared to pre-2009 system, banks' and their staff's responsibility for filing a report under article 9 is limited, but not non-existent.[443]

2.V.E. Tipping-off rules

The financial intermediary is prohibited from informing the person concerned or third parties of a required or permitted report it has filed.[444] A bank that breached its duty not to inform the persons concerned or third parties of a SAR may be subject to administrative sanctions specified in AMLA 1997. However, the act specified no measures against banking staff who inform the person concerned or third parties of a required or permitted report it has filed. Yet, banking staff commits an offence under Article 47 of Swiss Banking Act 1934 by tipping off. Article 47 of the act reads as follows:[445]

> 1. Whoever intentionally does the following shall be imprisoned up to three years or fined accordingly:
>
> a. discloses secret information entrusted to them in their capacity as a member of an executive or supervisory body, employee, representative or liquidator of a bank, as member of a body or employee of an audit firm or that they have observed in this capacity;
>
> b. attempt to induce an infraction of the professional secrecy;

[440] TF, 29 mars 2006, 4C.33/2006, cons. 3.1.
[441] Lombardini (n.356), 162.
[442] Ibid.
[443] Ibid.
[444] Article 10a, AMLA 1997.
[445] *Unofficial translation* (n.424).

c. disclose confidential information to third parties or use this information for own benefits or the benefit of others.

1[bis] . Whoever enriches themselves or others with an action in accordance with 1(a) or (c) shall be punished with imprisonment for up to five years or fined accordingly.

2. Whoever acts in negligence shall be penalised with a fine of up to CHF 250,000.

The legislator has taken measures not to inhibit information sharing required for the purposes of CDD and money laundering risk management within a financial group or between different institutions.[446]

2.V.F. Conclusion

This part showed that Swiss lawmakers gave effect to the FATF's STRs regime related recommendations by specifying high thresholds for a duty of reporting and mild sanctions to apply those who fail to comply with their duty of reporting.

2.VI. Conclusion

This thesis investigates AML laws relating to banks' duty and right to make SARs from the perspective of banking clients' right to the protection of personal data, and focuses on the recommendations adopted by the FATF and AML laws adopted by English and Swiss lawmakers. The SARs regime related AML rules are complicated (eg. there are different types of SARs that banks are required and/or permitted to make, there are some terms that needs to be clarified to understand the SARs regime), and many authors who work on criminal law, banking law or privacy laws related topics are not familiar with the SARs regime related AML rules that apply to the banks. By exploring relevant FATF recommendations and English and Swiss AML laws, this chapter clarified the rules that will be investigated from the perspective of banking clients' right to the protection of personal data.

This thesis focuses on the FATF's recommendations since the FATF is an inter-governmental organisation setting global standards for combatting money laundering. This chapter showed that the FATF recommends countries to impose by enforceable means on financial institutions duty to produce STRs where they suspect, or have reasonable grounds to suspect, that funds are the proceeds of crime.

This thesis compares English and Swiss AML laws to see different interpretations of the FATF's STRs regime related recommendations. This chapter showed that English law specified low thresholds for a duty of reporting and serious punishment terms to be applied to those who breached their duty of reporting. While Swiss legislator preferred relatively high thresholds and mild sanctions.

[446] Article 10a, AMLA 1997.

Information privacy laws with which AML rules that were subjected to an extensive comparative analysis should comply will be investigated in the following chapter.

CHAPTER 3: LAWS THAT PROTECT BANKING CLIENTS' RIGHT TO THE PROTECTION OF PERSONAL DATA

3.I. Introduction

Chapter 2 explored Anti-Money Laundering (AML) laws requiring and permitting banks to make suspicious transaction reports (STRs)/suspicious activity reports (SARs). This thesis aims to investigate relevant AML laws from the perspective of banking clients' right to the protection of personal data. This chapter examines legal mechanisms that protect banking clients' control rights over their personal data.

The FATF long remained silent on the subject of information privacy rights.[1] In 2018, the FATF advised countries to ensure compatibility of AML requirements with data protection and privacy rules.[2] However, the FATF has not yet explained what privacy and data protection rules to which its recommendation 2 refers.

In English and Swiss laws, data protection acts affect banking clients' right to the protection of personal data. Moreover, the law of confidence has long but partially protected banking clients' control rights over their personal data. Besides, English and Swiss AML laws that interfere with banking clients' information privacy rights should comply with Article 8-2 of the European Convention on Human Rights (ECHR).

3.II. Banking clients' right to the protection of personal data and the FATF's recommendations

3.II.A. Introduction

The FATF is an inter-governmental organisation that aims to set standards protecting the international financial system from the threat of money laundering.[3] The FATF long remained silent on information

[1] Privacy International, 'How financial surveillance in the name of counter-terrorism fuels social exclusion' 2019 <https://www.privacyinternational.org/long-read/3257/how-financial-surveillance-name-counter-terrorism-fuels-social-exclusion> 10 June 2021.
[2] Recommendation 2. FATF (2012-2020), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, 19, <www.fatf-gafi.org/recommendations.html> 10 June 2021.
[3] FATF (n.2), 7.

privacy laws because financial privacy was associated with crime.[4] Prior to 2018, recommendation 9 was the FATF's only recommendation where information privacy laws were referred to. Recommendation 9 aims to ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.[5]

In February 2018, the FATF revised its recommendation 2 and advised countries to ensure compatibility of AML requirements with data protection and privacy rules.[6] By virtue of recommendation 2, AML laws requiring and permitting banks to make STRs should comply with data protection and privacy rules. The FATF has not yet explained what data protection and privacy standards with which AML rules should comply.

3.II.B.The FATF's protracted silence on information privacy rights

Banks, banking staff and their clients can benefit from bank secrecy rules for good and evil. On the one hand, bank secrecy rules may help oppressed people in protecting their financial interests. For instance, article 47 of the Swiss Banking Act enabled German citizens with Jewish background to hide their wealth in Swiss banks from Nazis in the 1930s.[7] On the other hand, bank secrecy rules may help criminals in hiding their tainted money. For instance, strong secrecy laws in Switzerland arguably helped Nazis hide their illicit money after their defeat in World War II.[8] As Dr de Capitani, who was general counsel for Credit Suisse in the 1980s, explained more than 30 years ago, the bank secrecy concept may be referred to in two contradictory ways: a legal instrument that saved oppressed people's financial interests or a tool which offenders take benefit from.[9]

Some employ bank secrecy and privacy rights concerns to find supporters for regulations that are, in fact, economic profit-orientated only. A recent example where bank secrecy and privacy rights concerns were used for promoting a profit-orientated project may be the Swiss federal popular initiative "Oui à la protection de la sphère privée" (Yes to the protection of the private sphere).[10] The campaign page of

[4] D Neo, 'A Conceptual Overview of Bank Secrecy' in S Booysen and D Neo (eds), *Can Banks Still Keep a Secret?: Bank Secrecy in Financial Centres Around the World* (Cambridge University Press 2017), 5.
[5] Recommendation 9, FATF (n.2), 14.
[6] FATF website, "Outcomes FATF Plenary, 21-23 February 2018" <http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-february-2018.html> 10 June 2021.
[7] W de Capitani, 'Banking secrecy today' [1988] 10 U. Pa. J. Int'l. Bus. L. 57, 58-60.
[8] J T Kelly, 'United States Foreign Policy: Efforts to penetrate bank secrecy in Switzerland from 1940 to 1975' [1975] 6 Cal. W. Int'l L.J. 211, 211-213; R U Vogler, 'History' in Swiss Bankers Association's website. An extract taken from the '100 years of Swiss Banking. 100 people. 100 thank you', published for the 100th birthday of the SBA. <https://www.swissbanking.org/en/bankers-association/about-us/history> 10 June 2021.
[9] de Capitani (n.7), 57-58.
[10] See «Arrêté fédéral relatif à l'initiative populaire «Oui à la protection de la sphère privée» (Projet) », FF 2015 6467. for Federal Bill related to popular initiative "Yes to the protection of the private sphere" and « Initiative populaire fédérale «Oui à la protection de la sphère privée». Retrait » FF 2018 212 for withdrawal of the Bill.

this initiative, which opposed the limitation of bank secrecy in tax matters for the sake of privacy rights, did not bother to explain the reason why taxation cannot be a legitimate reason to limit bank clients' right to professional confidentiality, yet referred to Swiss banking secrecy's historical value at least once in each page.[11] Besides, tax-heavens and the FATF non-compliant countries often attempt to justify their position by referring to financial privacy and professional confidentiality.[12]

While some misuse bank secrecy and privacy rights concerns, some others demonised financial privacy and banking secrecy.[13] First, because bank secrecy and financial privacy are frequently employed by those who wish to justify tax-heavens, financial privacy within the banking context has mistakenly been associated with offshore states.[14] Second, a long list of cases where economic criminals and corrupted banking officials misused bank secrecy rules led to a confidentiality sceptic atmosphere. Indeed, journalists, politicians, officials of prominent international organisations and some authors associated bank secrecy and bank confidentiality with crime since the 1960s.[15]

Confidentiality or secrecy scepticism in the banking business went one step further after the 2008 financial crisis, as tax governance problems were attributed to strict financial secrecy laws. Officials of prominent international organisations and politicians preferred using anti-secrecy language to underline their position. For instance, the OECD started a process called "The era of bank secrecy is over",[16] while the FATF's former president Roger Vilkins AO attacked 'the privacy lobby', defending that the privacy lobby gives simple, rigid and ideological reactions against developing technology.[17] In the G20 2009 London summit, some politicians attacked bank secrecy and did not hesitate to use an aggressive

[11] Webpage of the popular initiative «Oui à la protection de la sphère privée»: <http://www.proteger-la-sphere-privee.ch/> 3 May 2020.
[12] M A Young, *Banking secrecy and offshore financial centers: Money laundering and offshore banking* (Routledge 2013), 21.
[13] Ibid.
[14] For instance, the telegraph writes "Offshore savers can kiss confidentiality goodbye" ('Offshore savers can kiss confidentiality goodbye' <https://www.telegraph.co.uk/finance/personalfinance/expat-money/8862417/Offshore-savers-can-kiss-confidentiality-goodbye.html> 10 June 2021), using the word confidentiality within banking context as an offshore practice only. Many further examples may be found in media (eg. 'Spilling secrets: the end of confidentiality in offshore financial centres' <https://www.lexology.com/library/detail.aspx?g=b1668640-55d0-4627-b95f-7999047328d4> 10 June 2021.).
[15] For instance, Masciandaro and Balakina defined banking secrecy in the second chapter of their book as "the use of the monetary, banking and financial services to hide the sources and/ or the destinations of money flow in order to reduce the probability of its complete identification." They defended that "in other words, banking secrecy is the device used to implement money laundering operations via the financial system." (D Masciandaro, O Balakina, *Banking Secrecy: Economics and Politics* (Palgrave Macmillan 2015), 6.
[16] OECD, 'The Era of Bank Secrecy is over; The G20/OECD Process is Delivering Results', 26 October 2011, <https://www.oecd.org/ctp/exchange-of-tax-information/48996146.pdf> 10 June 2021.
[17] Roger Vilkins AO, "The danger of driving both illicit markets and financial exclusion", remarks delivered at the 6th Annual International Conference on Financial Crime and Terrorism Financing, Kuala Lumpur, 8 October 2014, <http://www.fatf-gafi.org/publications/fatfgeneral/documents/danger-illicit-markets-financial-exclusion.html> 10 June 2021.

language against countries famous for their bank secrecy laws. Bank secrecy related debate at the summit was summarised by Steichen as follows:[18]

> Politicians of our neighbour countries did not mind either pilling additional pressure on Switzerland and Luxembourg. Indeed, Germany's former finance minister Peer Steinbrueck has been quoted as having said that countries should use 'the whip' on the Swiss to combat banking secrecy, while another German minister has waxed nostalgic about being able to send 'troops' into Luxembourg like in the good old days. Strong stuff, and Jean-Claude Juncker, prime minister of "tax haven" Luxembourg, told everyone interested in the matter that he did not find it funny.

Demonising 'bank secrecy' is not an issue exclusive to the English language. French term 'secret bancaire' has also been associated with crime by journalists and politicians. After the G20 meeting in London, Nicolas Sarkozy, former president of the Republic of France, stated that France fought to abate tax heavens, bank secrecy *(secret bancaire)* and organised fraud.[19] Whilst, 'secret bancaire' is a French term referring to banks' legal duty of secrecy recognised in article L. 511-33 of Monetary and Financial Code.

'Secrecy' and 'confidentiality' terms have been used interchangeably in legal literature.[20] Whilst, it is the bank secrecy term that has frequently been associated with crime by journalists and politicians. It is worth noting that there are examples where the confidentiality term was also associated with crime.[21]

---

[18] A Steichen, 'Information Exchange in Tax Matters: Luxembourg's New Tax Policy' in A Rust and E Fort (eds), *Exchange of information and bank secrecy* (Kluwer Law International 2012), 17.

[19] « […]A Londres, la France s'est battue pour que les paradis fiscaux, le secret bancaire, la fraude organisée, ça soit terminé. » N Cori, « Paradis fiscaux : Sarkozy rêve tout haut » Libération, 25 septembre 2009, <http://www.liberation.fr/france/2009/09/25/paradis-fiscaux-sarkozy-reve-tout-haut_583849> 10 June 2021.

[20] The European GDPR 2016/679, employ the term 'duty of professional secrecy' when it refers to 'obligation of confidentiality' in professional context. (See Articles 22 and 44(2) of the European GDPR.) Similarly, the Law Enforcement Directive 2016/680 employs the 'confidentiality of data protected by professional secrecy' expression several times. (Recitals 51 and 61 as well as article 44 of the European Law Enforcement Directive.) The European Court of Human Rights (ECtHR) used the expression of "confidentiality of exchanges between lawyers and their clients" while qualifying this protection as "professional secrecy" in the same decision (Eg. *Michaud v France* (2014) 59 E.H.R.R 9 at [118] ; and [121].). Moreover, the French term "un secret" is translated to English as "secret information" or "confidential information" in different resources. (The unofficial English translation of the Swiss Banking Act (Article 47) prepared by the KPMG Switzerland preferred the English term "confidential information" for the terms "un secret" and "Geheimnis" used in the original French and German texts of the Act respectively. (Unofficial translation of the Swiss Federal Act on Banks and Savings Banks (KPMG, 1 January 2016) 32 Available on https://assets.kpmg.com/content/dam/kpmg/ch/pdf/ch-banking-act-en.pdf) While the unofficial English translation of the French Penal Code (Article 226-13) provided in the Légifrance website - the official website of the French government for the publication of legislation, regulations, and legal information- translated the French term "un secret" as "secret information". (Unofficial translation of Penal Code, With the participation of John Rason Spencer QC, prepared in 1995 and updated 2005, 57 <https://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations> 21 January 2021.)

[21] See footnote 14 above. .

This secrecy or confidentiality sceptical environment affected legal literature too. Some researchers and practitioners argued that the presumption of secrecy needs to be replaced by a presumption of disclosure. Some others went further, arguing that bank secrecy is an outdated and useless concept.[22]

Within this secrecy-sceptical environment, the FATF, which was established in 1989 to set standards protecting the international financial system from the threat of money laundering long remained silent on information privacy laws. Prior to 2018, the FATF's only recommendation referred to information privacy rules was recommendation 9, which reads as follow: "Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations". The recommendation aimed to ensure that confidentiality laws do not inhibit implementation of the recommendations, did not advise countries to adopt laws that protect the information privacy rights of the clients of financial institutions.

3.II.C. FATF's recommendation 2

As explained above, bank secrecy and financial privacy are demonised in daily language. However, international human rights instruments require countries to protect individuals' data protection, privacy, and confidentiality rights.[23] The FATF did not remain unresponsive to data protection and privacy laws and integrated such laws into its' recommendation 2 in February 2018. Paragraph 2 of recommendation 2 reads as follows:[24]

> Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policymaking and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate and exchange information domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. This should include cooperation and coordination between relevant authorities to ensure the compatibility of AML/CFT/CPF

[22] Eg. see arguments defended by Mr. Kumar, Ms Hussein and Mr Moscow in the Thirteenth International Symposium on Economic Crime. 'The Thirteenth International Symposium on Economic Crime — Banking on Secrets: The Universal Balancing Act', (1996) 3(3) J.F.C. 223, 223-224.

[23] Examples of international instruments that require countries to protect individuals' right to the protection of personal data: the Council of Europe's Convention 108, the Charter of Fundamental Rights of the European Union and the OECD Data Protection Guidelines. By the end of 2018, there are more than 130 countries that have enacted data privacy laws. See G Greenleaf, 'Global Data Privacy Laws 2019: 132 National Laws & Many Bills' (2019) 157 *Privacy Laws & Business International Report* 14, 14-18. Moreover, the ECtHR recognised that bank clients' right to confidentiality falls under the scope of their Article 8 ECHR rights. (*M.N. v San Marino* (2016) 62 E.H.R.R. 19 at [51]).

[24] "CPF" term was added in October 2020. FATF's website (n.6).

requirements with Data Protection and Privacy rules and other similar provisions (e.g. data security/localisation).

Recommendation 2 clearly shows that the FATF, the international organisation that is establishing international AML standards since 1990, does not associate information privacy laws with economic crime. Au contraire, it advises relevant authorities to ensure AML rules' compatibility with data protection and privacy rules. Therefore, the FATF's amendment of its recommendation referring to Data Protection and Privacy rules is a significant step forward. However, it is worth mentioning that neither the recommendation nor interpretive note to recommendation explained what data protection and privacy standards to which the FATF refers.[25]

3.II.D. Conclusion

Bank secrecy and financial privacy terms were long associated with economic crime and money laundering. Therefore, the FATF, an inter-governmental organisation that is to set global standards protecting the international financial system from the threat of money laundering long remained silent on information privacy laws.

Several international human rights instruments adopted in the second half of the 20th century required lawmakers to protect banking clients' information privacy rights. The FATF did not remain unresponsive to these human rights instruments. In February 2018, the FATF revised its recommendation 2 and advised countries to ensure compatibility of AML requirements with data protection and privacy rules. The FATF's relevant reform showed that the international organisation that is establishing international AML standards does not associate information privacy laws with economic crime.

3.III. Banking clients' right to the protection of personal data in English and Swiss laws

The UK's Data Protection Act 2018 (DPA 2018) and Switzerland's Federal Act on Data Protection 1992 (FADP 1992) protect banking clients' right to the protection of personal data in the UK and Switzerland, respectively. Data protection acts require 'processing of personal data' to be in compliance with data protection principles and rights. The SARs often involve personal information[26] and disclosure by transmission amounts to data processing.[27] This means that making an STR often amounts

[25] Recommendation 2 and Interpretive Note to Recommendation 2. FATF (n.2), 10,37.
[26] The European Court of Human Rights held, in *M.N. v San Marino* (2016) 62 E.H.R.R. 19 at [51], that "information retrieved from banking documents undoubtedly amounts to personal data concerning an individual, irrespective of it being sensitive information or not".
[27] Most data protection acts define data processing as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, *disclosure by transmission*

to processing personal data. AML laws require and permit banks to make SARs to safeguard the prevention, investigation, detection and prosecution of criminal offences. Lawmakers can permit banks to interfere with their clients' data privacy rights by making SARs if the interference is prescribed by law, and such interference respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard the prevention, investigation, detection or prosecution of criminal offences. The reporting bank must still comply with some data protection rules.

Both English and Swiss laws impose upon banks and their staff a duty to confidentiality. The law of banking confidence has long but partially protected individual banking clients' control rights over their personal data. The law of confidence prohibits unauthorised disclosure of confidential information unless there is a legitimate reason for the disclosure, and personal information within a SAR often amounts to confidential information. Thus, the law of confidence permits banks to produce SARs under certain conditions.

Disclosure of personal and/or confidential data to a public authority without the data subject's or confider's consent may constitute an interference with respect for private life.[28] Accordingly, the SARs often interferes with banking clients' Article 8-1 ECHR rights. Laws requiring or permitting one to interfere with another's Article 8-1 rights must comply with Article 8-2. Therefore, relevant AML laws must comply with Article 8-2 ECHR. Both English and Swiss laws grant the Convention a privileged status. Thus, the SARs regime in both countries should be in compliance with Article 8 ECHR.

3.III.A. Data protection acts and the SARs produced by banks

This part investigates English and Swiss laws. Therefore, English Data Protection Act 2018 (DPA 2018), UK GDPR and Swiss Federal Act on Data Protection 1992 (FADP 1992) will be at the centre.

European Union (EU) law has largely influenced both English and Swiss data protection laws, while the UK exited the EU, and Switzerland has never been a member state. Directive on Data Protection 95/46/CE (Directive 95/46/CE) and the 2008 Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (Framework Decision 2008/977/JAI) enshrined data protection standards of the EU up until 2018. In order to comply with the Directive, Switzerland revised the Federal Act on Data Protection 1992 (FADP 1992) in 1998, while the UK Parliament enacted the Data Protection Act 1998, which superseded the Data Protection Act

[emphasis added], dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". (see Article 4, EU GDPR; and Article 3, the European Law Enforcement Directive).

[28] *Uzun v Germany* (2011) 53 E.H.R.R. 24, [47]; *Perry v the United Kingdom* (2004) 39 E.H.R.R. 3, [40]–[41].

1984. In 2016, the European Parliament ratified the European General Data Protection Regulation 2016/679 and the Law Enforcement Directive 2016/680, both of which are effective since 25 May 2018. The Regulation and Directive were to create a series of common standards for the whole of the EU.[29] While the Regulations are directly applicable in all member states, the Directives should be incorporated into national laws.[30] Accordingly, the UK Parliament replaced the DPA 1998 with the DPA 2018, which incorporated both the Regulation and Directive. Adoption of Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019/419 does not change the fact that DPA 2018 was largely influenced by the European General Data Protection Regulation 2016/679 and the Law Enforcement Directive 2016/680. On the other hand, the Swiss Federal Council outlined that it is economically important for Switzerland to be recognized as a country with an appropriate data protection level for the EU,[31] and drafted a Data Protection Bill in 2017,[32] which was largely influenced by the European GDPR. The legislative stage of the bill took much longer than expected. The Swiss Parliament approved the final draft on 25 September 2020. The Federal Council has not yet determined the Act's date of entry into force.[33] Federal Data Protection and Information Commissioner expects that the rev-DPA will enter into force in the course of 2022.[34] Therefore, this chapter will also refer to the European General Data Protection Regulation 2016/679 (European GDPR), the European Law Enforcement Directive 2016/680 (Law Enforcement Directive) and Switzerlands' revised Data Protection Act 2020 (rev-DPA 2020). Besides, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) [35] and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Data Protection Guidelines)[36] will be mentioned where necessary.

Both DPA 2018 and FADP 1992 apply to "the processing of personal data".[37] Banks' processing of personal data is not exempted from the ambit of these data protection acts.[38] Part 3.III.A.1 investigates the meaning of "processing of personal data" and defends that making an SAR often amounts to processing of personal data.

[29] Federal Data Protection and Information Commissioner FDPIC, 'The GDPR and its consequences for Switzerland' March 2018, 2.
[30] R Schutze, *European Union Law* (2nd edn, Cambridge 2018), 89-90, 114-115.
[31] Projet de loi, FF 2017 6803, 6871.
[32] Ibid.
[33] Article 74(2), rev-DPA 2020.
[34] Préposé fédéral à la protection des données et à la transparence, «Nouvelle loi fédérale sur la protection des données: le point de vue du PFPDT» 9 février 2021, 2.
[35] Article 2, the Convention 108.
[36] Article 1, OECD Data Protection Guidelines.
[37] In relation to the scope application of Part 2 of the DPA 2018, see section 4(2) of DPA 2018 and article 2 of the UK GDPR. In relation to the scope application of FAPD 1992, see Article 2(1) of the FADP 1992.
[38] In relation to the scope application of Part 2 of the DPA 2018, see section 4(2) of DPA 2018 and articles 2 and 4(6) of the UK GDPR. In relation to the scope application of FAPD 1992, see Article 2(2) of the FADP 1992.

Part 3.III.A.2.a explores data protection principles and rights. Part 3.III.A.2.b investigates data privacy rules apply where the processing of personal data is for the prevention and prosecution of crime.

3.III.A.1. The SARs and the ambit of Data Protection Acts

English and Swiss data protection acts apply to the processing of personal data. The SARs involve information relating to individual or corporate banking clients. Information relating to an individual amount to personal data according to the DPA 2018, while the FADP 1992's personal data definition embraces information relating to an individual or a legal person. Disclosure by transmission amounts to data processing. Therefore, making an SAR often amounts to processing of personal data.

Information within an SAR relating to a banking client, real or legal person, amounts to personal data for the purposes of FADP 1992. Therefore, all SARs involve personal information. It is worth mentioning that this position will change after the rev-DPA 2020's entry into force.[39]

Information within an SAR amounts to personal data for the purposes of DPA 2018 if it relates to an individual. In relation to their clients who are legal persons or arrangements, banks are required to understand the ownership and control structure of the customer. [40] They should identify "the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner." [41] SARs relating to corporate clients often involve information relating to the owners and directors of the reported client. Therefore, the SARs may involve personal information even where the reported client is a legal entity.

Personal data may be of private or public nature. Moreover, the way in which data was obtained by the data controller is not essential. As the ECtHR held in *M.N. v San Marino* "information retrieved from banking documents undoubtedly amounts to personal data concerning an individual, irrespective of it being sensitive information or not".[42] The SARs often involve the client's name, address, client number and banking transactions. Not only financial transaction data and client number but also name or address may amount to personal data. This is by no means that data protection laws do not consider the nature of data or confidentiality of data.

The EU's data protection instruments emphasised that the measures that interfere with data protection rights should take into account the risk to the rights and freedoms of natural persons.[43] The SARs regime

[39] See pages 95-96 below.
[40] Recommendation 10(4), The FATF Recommendations; (UK) Anti-Money Laundering Regulations 2017, Section 28 (3),(4); (CH) AMLA 1997, Article 3.
[41] Recommendation 10(4), The FATF Recommendations; (UK) Anti-Money Laundering Regulations 2017, Section 28 (4); (CH) article 4 of the AMLA 1997
[42] *M.N. v San Marino* (2016) 62 E.H.R.R. 19, [51], also see *Amann v. Switzerland* [GC], no. 27798/95, § 65, ECHR 2000-II.
[43] Eg. see Recital 75, EU GDPR 2016/679; Recital 51, the Law Enforcement Directive (EU) 2016/680.

interferes with the reported banking client's rights and freedoms more severely due to three reasons. First, the SARs interfere with the reported client's private life as they contain private information (eg. information relating to one's financial affairs such as financial transaction data). Second, bankers' reporting of SARs, which involve information that the confident banker obtained, observed or predicted in its' professional capacity, may harm the professional relationship of trust between the banker and its' client. Third, the SARs may trigger provisional measures that may give rise to financial loss and damage to the reputation of the reported person.[44]

3.III.A.1.a."Data processing" for the purposes of information privacy rights law literature

Legal scholars investigate the extent to which one ought to have legally protected information privacy rights and the way in which these rights should be given effect. As defended by European Data Protection Supervisor, "[t]he extent to which humans can enjoy their fundamental rights depends not only on legal frameworks and social norms, but also on the features of the technology at their disposal".[45] Therefore, data protection acts recognised the importance of data protection through technology design to protect information privacy rights. For instance, the European GDPR article 25 and the UK GDPR article 25 have incorporated privacy by design. Thus, information privacy is a research subject for not only legal scholars but also computer and data scientists who focus on the technical dimension of data protection. However, "data", "information" and "data processing" terms are employed in different senses by legal scholars and data science experts. This thesis follows the terminology employed in legal literature. When these terms are used as they are defined in data science, this will be particularly indicated.

3.II.A.1.a.i. "Data" and "information" terms

"Data" and "information" are two different terms in data science. Data refers to raw numbers and facts, while information accounts for processed data.[46] To put it another way, information is what results from

[44] See Recital 75, EU GDPR 2016/679; Recital 51, the Law Enforcement Directive (EU) 2016/680 and C Lombardini, *Banques et blanchiment d'argent* (3rd ed, Schulthess 2016), 157. relating to personal data processing of which interferes with the data subject's private life, personal data processing of which may give rise to financial loss, damage to the reputation or loss of confidentiality of data protected by professional secrecy.

[45] European Data Protection Supervisor, 'Preliminary Opinion on privacy by design', Opinion 5/2018 (31 May 2018) iii. <https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf> 10 June 2021.

[46] A Chandor, *The Penguin Dictionary of Computers* (Penguin books 1970), 99. A similar argument may be found in R W Cahn, *The Coming of Materials Science* (Elsevier 2011), 498.

the processing of data. Knowing this terminology may help legal scholars understand information technology better. However, it is worth mentioning that these terms have not always been used accordingly, even in data science. For instance, the very 'data mining' term is a misnomer as data mining is a process aiming at "the extraction of information from large amounts of data, not the extraction (mining) of data itself".[47]

Legal scholars use "data" and "information" terms interchangeably. Both terms refer to the knowledge provided, learned or extracted concerning some particular fact, subject, or event.[48] Complexity or production process of the knowledge is not essential for legal literature's definition of data or information. For instance, the European GDPR and the UK GDPR,[49] the European Law Enforcement Directive 2016/680,[50] the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108),[51] the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Data Protection Guidelines)[52] and the UK's DPA 2018,[53] employ these terms interchangeably defining personal data as any information relating to an identified or identifiable data subject. Similarly, the Swiss Federal Act on Data Protection 1992 (FADP 1992) employs the terms 'données' (data) and 'informations' interchangeably.[54]

There are some similarities between the definitions employed in data science and legal literature. First, both information privacy rights law and data science are interested in the very essence of knowledge, not in its' form. Therefore, knowledge preserved in any appropriate way may be qualified as data or information.[55] This means that data or information is not necessarily a printed document or structured in a particular format. Second, accuracy or truth is not an inherent element of legal literature's or data science's definition of data or information. Section 2 of the DPA 2018 and article 15 of FADP 1992[56] accept the possibility of the existence of inaccurate personal data by requiring "inaccurate personal data to be rectified". Information Commissioner's Office (ICO) stressed out that "if information seemingly relating to a particular individual is inaccurate (ie. it is factually incorrect or it is information about a

[47] Cahn (n.45), 498.
[48] Data is defined as "knowledge communicated concerning some particular fact, subject, or event" in Oxford English Dictionary, <http://www.oed.com/view/Entry/95568?redirectedFrom=information#eid> 10 June 2021.
[49] Article 4, the EU GDPR; article 4, the UK GDPR.
[50] Article 3, the European Law Enforcement Directive.
[51] Article 2, the Convention 108.
[52] Article 1, OECD Data Protection Guidelines.
[53] Section 3(2), DPA 2018.
[54] Article 3 of FADP 1992. Similarly, see article 5 of rev-DPA 2020.
[55] Data or information may be preserved as a photograph (*Pollard v Photographic Co* (1889) 40 Ch D 345; *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804, 807.), a drawing (*Nichotherm Electrical Co Ltd v Percy* [1957] RPC 207.) or a model (*Franklin v Giddings* [1978] 1 Qd R 72). For further information, see R Pattenden, *The Law of Professional-Client Confidentiality* (Oxford University Press 2003), 134; and H Fenwick and G Phillipson, 'Confidence and privacy: A Re-examination' (1996) 55 Cambridge L.J. 447, 450.
[56] See also article 32, rev-DPA 2020.

different individual), the information is still personal data, as it relates to that individual".[57] Similarly, Longmore LJ in *McKennit v Ash* [2008] explained irrelevancy of truth for information privacy laws as follows: "[t]he question in a case of misuse of private information is whether the information is private not whether it is true or false. The truth or falsity of the information is an irrelevant inquiry in deciding whether information is entitled to be protected".[58]

3.III.A.1.a.ii. Data processing

Data processing is defined in data science as "the collection or manipulation of items of data to produce meaningful information".[59] Hence, processing covers collection and manipulation activities that are aimed at producing new information. Mere recording, disclosure by transmission, anonymisation or destruction does not amount to data processing.

Legal literature adopted a significantly broader definition. Processing comprises any operation or set of operations performed on information. For instance, the European GDPR and Law Enforcement Directive define "processing" as

> "any operation or set of operations whether or not by automated means, […] such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[60]

The Convention 108,[61] DPA 2018[62] and FADP 1992[63] have also adopted very similar definitions for the term "processing". Thus, not only "the collection or manipulation of items of data to produce meaningful information" (eg. profiling, structuring and combination etc.) but also other types of operations which are not to extract further information (eg. disclosure by transmission, erasure, destruction and anonymisation) are accepted as data processing in legal literature.

[57] ICO website, What ist the meaning of 'relates to'? <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-the-meaning-of-relates-to/> 10 June 2021.
[58] *McKennit v Ash* [2008] QB 73 by Longmore LJ.
[59] C S French, *Oliver and Chapman's Data Processing and Information Technology* (10th edn, Thomson 2004), 2.
[60] Article 4, EU GDPR; and Article 3, the European Law Enforcement Directive. See also article 4, UK GDPR.
[61] Article 2, the Convention 108.
[62] Section 3(4), DPA 2018.
[63] Article 3 of FADP 1992. See also article 5, rev-DPA 2020.

3.III.A.1.b. Personal data

European data protection instruments (ie. the European GDPR,[64] European Law Enforcement Directive,[65] Council of Europe Convention 108[66] and the OECD Data Protection Guidelines[67]) define personal data as "any information relating to an identified or identifiable natural person". International instruments "should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties".[68] Therefore, they should not be interpreted as impeding more robust privacy protection. The Convention 108, for instance, explicitly states that any state may apply "this Convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality".[69] Therefore, there may be different 'personal data' definitions in different legal systems. This chapter will investigate the personal data definitions adopted in English and Swiss laws.

DPA 2018 defines personal data as "information relating to an identified or identifiable individual".[70] Accordingly, "information about a limited company or another legal entity, which might have a legal personality separate to its owners or directors, does not constitute personal data".[71] However, data protection rules does apply

> to personal data relating to individuals acting as sole traders, employees, partners, and company directors wherever they are individually identifiable and the information relates to them as an individual rather than as the representative of a legal person. A name and a corporate email address clearly relate to a particular individual and is therefore personal data. However, the content of any email using those details will not automatically be personal data unless it includes information which reveals something about that individual, or has an impact on them.[72]

The FADP 1992 defines personal data as "information relating to an identified or identifiable person".[73] Hence, it applies to data relating to real or legal persons. Following the EU GDPR, the Swiss Federal

[64] Article 4, the EU GDPR.
[65] Article 3, the European Law Enforcement Directive.
[66] Article 2, the Convention 108.
[67] Article 1, OECD Data Protection Guidelines.
[68] Article 6 of the OECD Data Protection Guidelines
[69] Art 3 of the Council of Europe Convention 108.
[70] Section 3(2), DPA 2018. DPA 1998 had the same definition for 'personal data' in its' section 1.
[71] ICO website, "What is personal data?" <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/> 10 June 2021.
[72] Ibid.
[73] Article 3, FADP 1992.

Council decided to change the FADP 1992's personal data definition. Rev-DPA incorporates personal data definition in the European GDPR.[74]

Data which relates to an identified or identifiable data subject constitutes personal data. An identifiable natural person refers to

> one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[75]

Personal data that have undergone pseudonymisation should be considered to be information on an identifiable natural person.[76] This is because it could be attributed to a natural person by the use of additional information. Yet, personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable does not amount to personal data.[77] It is worth mentioning that anonymisation of personal data constitutes personal data processing because data is personal data before the anonymisation, and anonymisation amounts to processing of data.[78]

3.III.A.2. Data subjects' *prima facie* control rights over their personal data

3.III.A.2.a. Data protection principles and rights

Data protection acts give effect to individuals' right to the protection of personal data by laying down rules relating to the protection of data subjects with regard to the processing of personal data.[79] Data protection acts give data subjects some control rights over their personal data, making them master of their personal data. Data protection acts recognise that data protection principles and rights may be limited for the prevention and prosecution of crime.

The principles and rights in the UK GDPR are integrated into English data protection law. Part 2 of DPA 2018, which "applies to the types of processing of personal data to which the UK GDPR applies

[74] The rev-DPA defined personal data as "information relating to an identified or identifiable real person". (Article 5, rev-DPA 2020, https://www.parlament.ch/centers/eparl/curia/2017/20170059/Texte%20pour%20le%20vote%20final%203%20NS%20F.pdf). Some scholars and federal authorities criticised this. For a detailed discussion of this subject, see «Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales», 10 Aout 2017, 9-11 <https://www.admin.ch/ch/f/gg/pc/documents/2826/Revision-totale-de-la-loi-sur-la-protection-des-donnees_Rapport-resultats_fr.pdf> 10 June 2021.
[75] Article 4 of the Regulation and Article 3 of the Directive.
[76] The European GDPR Recital 26.
[77] The European GDPR Recital 26.
[78] D Beyleveld and E Histed, 'Betrayal of Confidence in the Court of Appeal' (2000) 4 Med.L.Int. 277, 292.
[79] Eg. see Article 1, the European GDPR; section 2(1) DPA 2018.

by virtue of Article 2 of the UK GDPR, … supplements, and must be read with, the UK GDPR."[80] Hence, it is DPA 2018 and the UK GDPR that concretised data subject's control rights over their personal data in relation to general processing by adopting data protection principles and rights.

The FADP 1992 concretised data subject's control rights over their personal data by adopting data protection principles and rights. The Ordinance on the Federal Act on Data Protection 1993 (Ordinance 1993) sets out the specifics of Swiss law's data protection principles and rights. Moreover, FADP 1992, a federal act, should be in compliance with the federal constitution.

Data protection laws give data subjects *prima facie* control rights over their personal data. First, data protection laws limit circumstances in which third parties are permitted to process personal data. Second, where a third party is permitted to process personal data, the data subject is still entitled to some control rights. Third, data processors are required to take some measures to abstain from breaching the freedoms and rights of data subjects.

Data protection laws limit circumstances where others are permitted to process data relating to a data subject. The UK GDPR concretised this by adopting the principles of lawfulness and fairness,[81] purpose limitation, [82] data minimisation[83] and storage limitation [84] in addition to recognising data subjects' right to erasure ('right to be forgotten'),[85] right to restriction of processing,[86] right to object[87] and "right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her",[88] and right to be provided with information by the data controller which obtained personal data from the data subject or from another source.[89] The FADP 1992 also limits circumstances where others are permitted to process data relating to a data subject. The FADP 1992 adopted the principles of lawfulness, proportionality and purpose limitation.[90] According to article 4(4), "[t]he collection of personal data and in particular the purpose of its processing must be evident to the data subject." Moreover, the Federal Act imposed

[80] Article 4(2), DPA 2018.
[81] Article 5(1)a, UK GDPR; see also Article 5(1)a, European GDPR.
[82] Article 5(1)b, UK GDPR; see also Article 5(1)b, European GDPR.
[83] Article 5(1)c, UK GDPR; see also Article 5(1)c, European GDPR.
[84] Article 5(1)e, UK GDPR; see also Article 5(1)e, European GDPR.
[85] Article 17, UK GDPR; see also Article 17, European GDPR.
[86] Article 18, UK GDPR; see also Article 18 of the European GDPR.
[87] Article 21, UK GDPR; see also Article 21 of the European GDPR
[88] Article 22, UK GDPR; see also Article 22 of the European GDPR.
[89] Articles 13 and 14 of UK GDPR.
[90] Article 4 of FADP 1992 reads as follows:
1 Personal data may only be processed lawfully.
2 Its processing must be carried out in good faith and must be proportionate.
3 Personal data may only be processed for the purpose indicated at the time of collection, that is evident from the circumstances, or that is provided for by law.
4 The collection of personal data and in particular the purpose of its processing must be evident to the data subject.
5 If the consent of the data subject is required for the processing of personal data, such consent is valid only if given voluntarily on the provision of adequate inforrmation. Additionally, consent must be given expressly in the case of processing of sensitive personal data or personality profiles.

upon data controllers duty to provide information on the collection of sensitive personal data and personality profiles.[91] Article 3(1) of the Act defined sensitive personal data and personality profiles as follows:

> c. *sensitive personal data*: data on:
>
> 1. religious, ideological, political or trade union-related views or activities,
>
> 2. health, the intimate sphere or the racial origin,
>
> 3. social security measures,
>
> 4. administrative or criminal proceedings and sanctions;
>
> d. *personality profile:* a collection of data that permits an assessment of essential characteristics of the personality of a natural person.

It is worth noting that an SAR may involve sensitive personal data (eg. trade union-related views or activities, social security measures, sanctions etc.) and personality profile.[92] Furthermore, the FADP 1992 provides a particular protection for confidential, sensitive personal data and personality profiles. According to article 35 of the FADP 1992,

> 1 Anyone who without authorisation wilfully discloses confidential, sensitive personal data or personality profiles that have come to their knowledge in the course of their professional activities where such activities require the knowledge of such data is, on complaint, liable to a fine.
>
> 2 The same penalties apply to anyone who without authorisation wilfully discloses confidential, sensitive personal data or personality profiles that have come to their knowledge in the course of their activities for a person bound by professional confidentiality or in the course of training with such a person.
>
> 3 The unauthorised disclosure of confidential, sensitive personal data or personality profiles remains an offence after termination of such professional activities or training.

Where a data processor is permitted to process personal data, the data subject is still entitled to some control rights. Both UK GDPR and the FADP 1992 accept the principle of transparency[93] and recognise data subject's right of access[94] and right to rectification.[95] Besides, UK GDPR acknowledges data subjects' right to data portability.[96]

[91] Article 14 of the FADP 1992.
[92] O Audouin, La Lutte Anti Blanchiment dans la Banque (Afges 2007), 67.
[93] Article 5(1)a of UK GDPR and Article 4(4) of the FADP 1992.
[94] Articles 15 of UK GDPR and article 8 of the FADP 1992.
[95] Articles 16 of UK GDPR, and article 5 of the FADP 1992.
[96] Article 20 of UK GDPR.

Data processors are required to take measures to abstain from breaching freedoms and rights of data subjects. UK GDPR adopted the principles of fairness,[97] accuracy,[98] integrity and confidentiality[99] and accountability.[100] Similarly, the FADP 1992 adapted accuracy[101] and security[102] principles and require processing to be carried out in good faith.[103]

3.III.A.2.b. The prevention and detection of crime and data protection acts

3.III.A.2.b.i. The UK's DPA 2018

According to article 23 of UK GDPR,

> 1 The Secretary of State may restrict the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:
>
> …
>
> (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
>
> …
>
> 2 In particular, provision made in exercise of the power under paragraph 1 shall contain specific provisions at least, where relevant, as to:
>
> …
>
> (d) the safeguards to prevent abuse or unlawful access or transfer;
>
> …
>
> (h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

[97] Article 5(1)a, UK GDPR.
[98] Article 5(1)d, UK GDPR.
[99] Article 5(1)f, UK GDPR.
[100] Article 5(2), UK GDPR.
[101] Article 5 of the FADP 1992.
[102] Article 7 of the FADP 1992.
[103] Article 4(2) of the FADP 1992.

Part 1 of Schedule 2 of the DPA 2018 "makes provision adapting or restricting the application of rules contained in Articles 13 to 21 and 34 of the UK GDPR in specified circumstances, of a king described in Article 6(3) and Article 23(1) of the UK GDPR".[104] According to section 5(2) of Schedule 2,[105]

> The listed GDPR provisions do not apply to personal data where disclosure of the data is required by an enactment, a rule of law or an order of a court or tribunal, to the extent that the application of those provisions would prevent the controller from making the disclosure.

According to section 1 of Schedule 2, the listed GDPR provisions to which section 5 of Part 1 of Schedule 2 is referring cover:[106]

> (a)the following provisions of the UK GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the UK GDPR)—
>
> (i)Article 13(1) to (3) (personal data collected from data subject: information to be provided);
>
> (ii)Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);
>
> (iii)Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);
>
> (iv)Article 16 (right to rectification);
>
> (v)Article 17(1) and (2) (right to erasure);
>
> (vi)Article 18(1) (restriction of processing);
>
> (vii)Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);
>
> (viii)Article 20(1) and (2) (right to data portability);
>
> (ix)Article 21(1) (objections to processing);
>
> (x)Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in sub-paragraphs (i) to (ix); and
>
> (b)the following provisions of the UK GDPR (the application of which may be adapted by virtue of Article 6(3) of the UK GDPR)—
>
> (i)Article 5(1)(a) (lawful, fair and transparent processing), other than the lawfulness requirements set out in Article 6;
>
> (ii)Article 5(1)(b) (purpose limitation).

[104] Section 15(2), DPA 2018.
[105] Section 5(2) of Part 1 of Schedule 2 of DPA 2018
[106] Section 1 of Part 1 of Schedule 2 of DPA 2018

Hence, if an enactment requires the data controller to make disclosure, above-listed provisions of the UK GDPR do not apply to the extent that the application of those provisions would prevent the controller from making the disclosure. The POCA 2002 requires banks to make disclosure.[107] Therefore, by virtue of section 5 of Part 1 of Schedule 2, above-listed provisions do not apply to the extent that the application of those provisions would prevent the banks from making disclosure.

Section 1 of Part 1 of Schedule 2 underlined that the lawfulness requirements set out in Article 6 of the UK GDPR are not amongst the listed provisions.[108] Therefore, lawfulness requirements set out in Article 6 would still apply to the banks upon whom POCA 2002 imposed a duty to make disclosure under certain conditions.

According to article 6(1)c of the UK GDPR, processing shall be lawful if and to the extent that processing is necessary for compliance with a legal obligation to which the controller is subject. Article 6(3) established that the basis for the processing referred to in point (c) of paragraph 1 shall be laid down by domestic law. "The purpose of the processing shall be determined in that legal basis…. The domestic law shall meet an objective of public interest and be proportionate to the legitimate aim pursued."[109]

POCA 2002 is the domestic law that imposed the duty of reporting to which banks are subject. Therefore, relevant sections of POCA 2002 "shall meet an objective of public interest and be proportionate to the legitimate aim pursued".[110] The objective of the relevant sections of POCA 2002 is the detection, prevention and prosecution of crime.

3.III.A.2.b.ii. Switzerland's FADP 1992

Article 13(2) of the Federal Constitution of the Swiss Confederation recognises everyone's "right to be protected against the misuse of their personal data". Article 35 of the Federal Constitution recognises the vertical and horizontal applicability of fundamental rights. Moreover, according to article 36 of the Federal Constitution,

> 1 Restrictions on fundamental rights must have a legal basis. …
>
> 2 Restrictions on fundamental rights must be justified in the public interest or for the protection of the fundamental rights of others.
>
> 3 Any restrictions on fundamental rights must be proportionate.
>
> 4 The essence of fundamental rights is sacrosanct.

[107] See sections 327-331, and 338 of POCA 2002.
[108] Section 1(b)i of Part 1 of Schedule 2 of DPA 2018.
[109] Section 6(3) of the UK GDPR, similarly see section 6(3) of the EU GDPR.
[110] Section 6(3) of the UK GDPR.

Hence, any law that justifies a breach of the right to the protection of personal data must be justified in the public interest or for the protection of the fundamental rights of others, must be proportionate and must not touch upon the essence of the right to be protected against the misuse of their personal data. Articles 305bis and 305ter of Swiss Criminal Code 1937 and articles 9 and 11 of AMLA 1997 lay out rules relating to bankers' duty and privilege to interfere with their clients' data protection rights by producing SARs. Relevant rules must be proportionate to the prevention or prosecution of crime and must not touch upon the essence of the right to be protected against the misuse of their personal data.

According to the FADP 1992,[111]

> 1 Personal data may only be processed lawfully.
>
> 2 Its processing must be carried out in good faith and must be proportionate.
>
> 3 Personal data may only be processed for the purpose indicated at the time of collection, that is evident from the circumstances, or that is provided for by law.
>
> 4 The collection of personal data and in particular the purpose of its processing must be evident to the data subject.
>
> …

Hence, banks can lawfully share their suspicions with competent authorities the extent to which it is necessary and proportionate to comply with a legal obligation to which they are subject.

Data subjects' rights recognised in articles 8 and 14 can be limited in compliance with article 9.[112] According to article 9, "The controller of a data file may refuse, restrict or defer the provision of information where: a. a formal enactment so provides; b. this is required to protect the overriding interests of third parties." Formal enactment term refers to "1. federal acts, 2. decrees of international organisations that are binding on Switzerland and international treaties containing legal rules that are approved by the Federal Assembly".[113] Such federal acts should comply with the Federal Constitution.

The financial intermediary is prohibited from informing the person concerned or third parties of a required or permitted report it has filed.[114] A bank that breached its' duty not to inform the persons concerned or third parties of a SAR may be subject to administrative sanctions specified by AMLA 1997. Moreover, banking staff commits an offence under Article 47 of Swiss Banking Act 1934 by tipping off. Once the report has been filed, the reporting person is prohibited from tipping off without a time limit. Where reported persons' relevant rights, including right to be provided with information

[111] Article 4, FADP 1992.
[112] Article 8 is on data subjects' right to information. Article 14 imposes upon the data controller Duty to provide information on the collection of sensitive personal data and personality profiles.
[113] Article 3 FADP.
[114] Article 10a, AMLA 1997.

and right of access are restricted, such limitation should be in compliance with the constitutional principles enshrined in article 36 of the Federal Constitution.

3.III.A.3. Conclusion

In English and Swiss laws, data protection acts protect banking clients' right to the protection of personal data. Some dispositions of the data protection acts apply to the processing of personal data by a bank even where the bank's processing of personal data is to comply with a legal duty to which the bank is subject. Lawmakers can legitimately permit and require banks to interfere with their client's right to the protection of personal data where the interference is necessary and proportionate to the detection, prevention and prosecution of crime.

3.III.B. Law of confidence and the SARs produced by banks

Developing technology in the 19th century enabled private and public persons to obtain and use others' personal and commercial secrets to an unprecedented extent for that time. As a response, lawmakers adopted privacy and confidentiality laws to protect individuals' information privacy rights.

In mid-19th century's England, law of confidence was frequently used to accommodate "individuals' concerns to retain a sphere of personal control over information of a personal and professional character in a complex urbanized society".[115] Prior to early 20th century, there was so little authority as to the banks' duty to keep customers, or clients' affairs secret[116] and the courts were reluctant to recognise a legal duty of confidentiality owed by banks to their customers.[117] The Court of Appeal recognised banks' contractual duty of secrecy in *Tournier v. National Provincial and Union Bank of England* in 1924.[118]

[115] M Richardson et al, *Breach of Confidence: Social Origins and Modern Developments* (Edward Elgar 2011), 33.
[116] *Tournier v. National Provincial and Union Bank of England* (1924)1 KB 461, at 479 (by Scrutton L.J.)
[117] R Stokes, 'The Banker's Duty of Confidentiality' (PhD thesis, University of Liverpool 2005),15.
[118] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B. 461.

Bank secrecy found its' legal basis in Swiss federal law with the adoption of Civil Code 1907 and Code of Obligations 1911.[119] Prior to these acts, there were no more than some cantonal laws which imposed banks a duty of confidentiality.[120]

Banks' duty of professional confidentiality, particularly its' economic crime prevention related limits, is an appealing international and comparative law subject. This is because an effective fight against economic crime committed in the banking sector requires establishing a strong international co-operation, as banking services and, therefore, the crimes misusing them, have largely been globalised. Several international organisations produce regular mutual evaluation reports concerning bank secrecy laws in their member countries,[121] and there are many comparative law books, book chapters and articles in addition to several regular or ad-hoc international events focused on the scope and limits of banks' duty of confidentiality.[122] Therefore, bankers' legal duty of confidentiality gained a globally accepted international definition. According to this definition, law of confidence prohibits misuse (unauthorised use to the detriment of the confider) or unauthorised disclosure of confidential information by the banker.[123] Moreover, confidential information is defined as data of confidential nature which has been acquired by the banker in circumstances importing an obligation of banking confidence.[124]

---

[119] H Bollmann and P Gmuer, 'Switzerland' in D Campbell (ed), *International Bank Secrecy* (Sweet & Maxwell 1992), 665; P S Grassi and D Calvarese, 'The duty of confidentiality of banks in switzerland: where it stands and where it goes. Recent developments and experience. The swiss assistance to, and cooperation with the italian authorities in the investigation of corruption among civil servants in italy (the "clean hands" investigation): how much is too much? ' (1995) 7 Pace Int'l L.Rev. 333; M Naim, «Eléments du droit comparé pour renforcer le secret bancaire» (PhD Thesis, Université Catholique de Louvain 1982), 231; O Dunant and M Wassmer, 'Swiss Bank Secrecy: its Limits under Swiss and International Laws' (1988) 20(2) Journal of International Law 543; F Chaudet «L'obligation de diligence du banquier en droit privé» (1994) Swiss Law Review 20; S Guex, «Les origines du secret bancaire suisse et son rôle dans la politique de la Confédération au sortir de la Seconde Guerre mondiale ». In: Genèses, 34, 1999. Varia. 5.

[120] eg. Laws of commerce laid down by the Great Council of Geneva in 1713. Naim (119), 178. If Articles 392-405 of the Federal Code of Obligations 1881, where the duties of contractual agents towards their principles are determined, were interpreted as articles 394-398 of the Code of Obligations 1911 is now interpreted, it would have been possible to argue that bank secrecy found its' basis in federal law with the adoption of the Federal Code of Obligations 1881. However, at the time, no one argued for such interpretation. Swiss Code of Obligations 1881, <https://www.amtsdruckschriften.bar.admin.ch/viewOrigDoc.do?id=10066139> 10 June 2021

[121] Eg. Annual country reports and financial secrecy index produced by Tax justice network and compliance with recommendation 9 part of the FATF's Mutual Evaluation Reports.

[122] Some of the most recent examples may be S Booysen and D Neo (eds), *Can Banks Still Keep a Secret?: Bank Secrecy in Financial Centres Around the World* (Cambridge University Press 2017) and G Godfrey and F Neate (eds), *Neate and Godfrey: Bank Confidentiality* (Bloomsbury 2015). See also University of Cambridge Thirteenth International Symposium on Economic Crime— Banking on Secrets: The Universal Balancing Act" Cambridge, 1995.

[123] The court in *Hardy v Veasey* [1868] LR 3 Ex. 107, 112 did not see loss of secrecy of private facts *per se* as damage. To avoid any misunderstanding, this thesis uses "misuse of information" and "unauthorised disclosure of confidential information" separately, while the former should include the latter.

[124] Eg. authors in K Hinterseer, *Criminal Finance – The political economy of money laundering in a comparative legal context* (Kluwer Law International 2002); E U Savona, *Responding to money laundering – international perspectives* (Harwood academic publishers 1997), Part II; have all adopted this basic definition for confidential information.

Compared to data protection laws, law of confidence provides limited protection for data subjects' control rights over their personal data. First, confidential data does not cover all personal data. Second, law of confidence prohibits misuse or unauthorised disclosure of protected information, while data protection laws require any and all processing of personal data to be in compliance with some principles and rights. The scope of application of the law of confidence and personal data protection laws, therefore, can be compared with a two-dimensional analysis: data protected (confidential data v personal data) and types of prohibited or regulated acts (misuse or unauthorised disclosure v any data processing.)

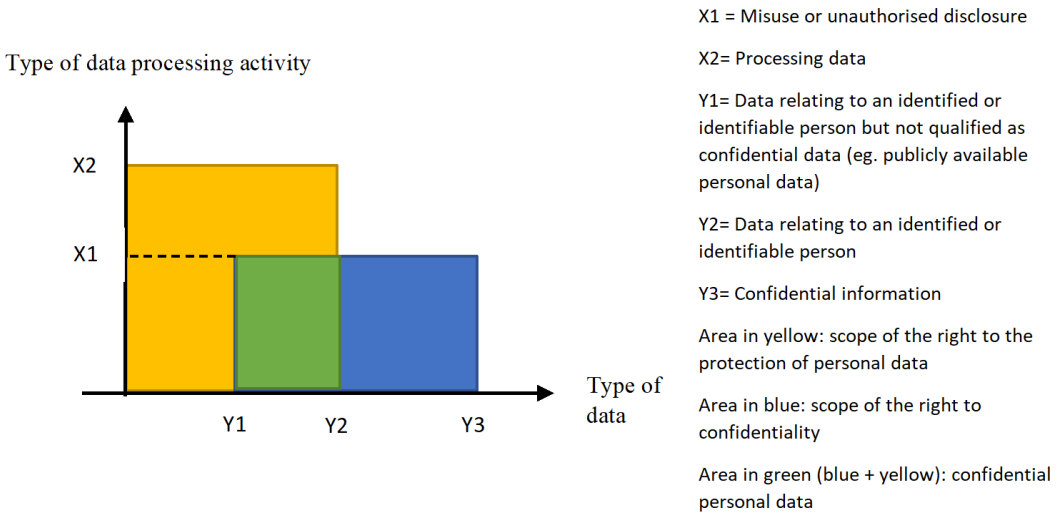


Chart 6: Data protection acts' and law on confidence's scope of application

Circumstances where law of banking confidence applies and circumstances where data protection laws apply constitute two intersecting sets. Law of confidence is engaged with when the confider discloses without the permission of the confider or misuses "confidential information", while data protection laws apply to "the processing of personal data".

Banking data that makes the bank suspect that its client's funds are or represent proceeds of crime often amounts to private information. Moreover, the bank obtains such information often in circumstances importing an obligation of banking confidence. Therefore, personal data within an SAR often amount to confidential information. Because law of confidence prohibits unauthorised disclosure of confidential data unless some conditions are met, banks' SARs breach law of confidence unless such conditions are met.

This part will first explain what types of acts on confidential information are prohibited by law of confidence. Afterwards, confidential information will be defined. Lastly, the limits of the prohibition of unauthorised disclosure will be investigated.

3.III.B.1. Bankers' legal duty of secrecy: prohibition of unauthorized disclosure

Law of confidence prohibits unauthorised disclosure or misuse of confidential information. This thesis investigates unauthorised disclosure because its focus is banks disclosure of banking information to the FIUs.

3.III.B.1.a. Prohibition of unauthorized disclosure of confidential information in common law: bankers' contractual and equitable duty of secrecy

English law relating to the breach of banking confidence is co-governed by contract and equity law principles.[125] Equity plays a complementary role and apply to banks' non-contractual professional relations.[126]

In *Hardy v Veasey* in 1868, Martin B recognised that bankers are under a duty not to use customer's data to the damage of the customer. However, his lordship did not see the loss of secrecy of private facts as damage *per se*.[127] Some 56 years after *Hardy v Veasey*, the Court of Appeal, in *Tournier v National Provincial and Union Bank of England*, held that "[…] one of the implied terms of the [banking] contract is that the bank enters into a qualified obligation with their customer to abstain from disclosing information as to his affairs without his consent."[128] Hence, the Court of Appeal recognised bankers' contractual duty to keep their clients' confidential information secret.

Equitable law of confidentiality, from which misuse of private information tort has been created, is more complicated than the contractual duty of confidentiality. Megarry J, in *Coco v A.N. Clark (Engineers) Limited*, explained three elements that are normally required if, apart from contract, a case of breach of confidence is to succeed as follows:[129]

> First, the information itself, in the words of Lord Greene, M.R. in the *Saltman* case … must "have the necessary quality of confidence about it". Secondly, that information must have

[125] R Cranston, *Principles of Banking Law* (Second edn, OUP 2002) 169, 171.
[126] R P Meagher, J D Heydon, M J Leeming, *Meagher, Gummow and Lehane's equity, doctrines, and remedies* (4th edition, Sydney 2002), [41-020]; see also Pattenden (n.55), 144.
[127] *Hardy v Veasey* [1868] LR 3 Ex. 107, 112. See 3.II.A above.
[128] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B. 461
[129] Coco v A N Clark (Engineers) Limited (1969) PRC 41, 47.

been imparted in circumstances importing an obligation of confidence. Thirdly, there must be an unauthorised use of that information to the detriment of the party communicating it.

As Fenwick and Phillipson explained, "subsequent case law suggests either that unwanted revelation of private facts *per se* may constitute detriment for the purposes of the law of confidence, or, alternatively, that detriment might not always be necessary".[130] Therefore, the first two elements became the key elements of the modern action for equitable breach of confidence.[131] Hence, the confidant is under a *prima facie* duty not to disclose confidential information without the authorization of the confider.

Contractual duty of confidentiality arises when the confidant acquires data of confidential nature within a contractual relationship of confidence.[132] Banks owe their clients an equitable duty of secrecy if the information has the necessary quality of confidence about it, and it has been imparted in the circumstances importing an obligation of confidence.

3.III.B.1.b. Prohibition of unauthorized disclosure of confidential information in Swiss federal law: Article 47 of the Banking Act, Article 28(1) of the Civil Code and Articles 394-398 of the Code of Obligations

Banks' legal duty of secrecy in Swiss law has three legislative bases at the federal level: Article 47 of the Federal Act on Banks and Savings Banks 1934 (FABSB 1934), Article 28(1) of the Civil Code, and Articles 394-398 of the Code of Obligations. Although some scholars add to this list Article 273 of the Criminal Code, industrial espionage, it would be difficult to support this argument since the scope of the information protected and the nature of the protection provided is significantly different.[133]

Article 47 of the FABSB 1934, where an intentional or negligent breach of bank secrecy is set forth as a criminal offence, applies to whom secret information is entrusted "in their capacity as a member of an executive or supervisory body, employee, representative or liquidator of a bank, as member of a body or employee of an audit firm or that they have observed in this capacity". Hence, this article applies to all types of financial products and services provided by banks and audit firms. Banking staff who intentionally reveal a secret entrusted to him in his capacity as a banker or observed by him in his professional capacity may be prosecuted with a prison term of three years and/or a fine. If the author of the breach acted in negligence, he is subject to a fine only. It is worth mentioning that before 2015,

[130] See A-G v Guardian Newspapers (No. 2) (1990) 1 AC 109 and H Fenwick and G Phillipson, *Media Freedom under the Human Rights Act* (OUP 2010), 728.
[131] T Aplin et al, *Gurry on Breach of Confidence: The Protection of Confidential Information* (2nd edn, OUP 2012) at [2.129].
[132] Pattenden (n.55), 100.
[133] Bollmann and Gmuer (n.119), 663.

Article 47 had penalised confidential information's unauthorised disclosure only. Since 2015, not only unauthorised disclosure but also unauthorised use of confidential data constitutes an offence.

Article 28(1) of the Civil Code 1907 provides legal protection against any infringement of natural and legal persons' personality rights. The Federal Supreme Court recognised that one's personality rights comprise, among others, one's privacy rights, including one's right to keep his financial affairs and personal fortune secret.[134] Therefore, Article 28(1) of the Civil Code can be applied to breach of bank secrecy cases. Articles 28-30 of the Civil Code provides judicial injunctions against the infringements of the personality rights of natural or legal persons. Moreover, breach of Article 28(1) constitutes a tort under Article 41 of the Code of Obligations.[135]

Default rules related to contractual agents' duties towards their principles listed in Articles 394-398 of the Code of Obligations 1911 constitute a contract law basis for bankers' duty of confidentiality. In a contractual agency relation, "unless expressly defined by the contract, the scope of the agency is determined by the nature of the business to which it relates",[136] and "the agent is liable to the principal for the diligent and faithful performance of the business entrusted to him".[137] According to the Tribunal Federal, diligent and faithful performance of banking service considering the nature of the banking business requires a duty to keep their clients' confidences secret.[138] Thus, banking contracts which contain elements of a contractual agency relationship impose bankers a duty of confidentiality.[139] Alternatively, article 398(1) disposes that "the agent generally has the same duty of care as the employee in an employment relationship". Accordingly, employee's duty of confidentiality in article 321a[140] can be applied to contractual agents as long as it is appropriate for the nature of the business.[141] Therefore, a client can bring an action for breach of contract against his bank who reveals confidential information.

3.III.B.2. 'Confidential information' for the purposes of bankers' duty of secrecy

Law of confidence prohibits unauthorised disclosure of confidential information. Confidential information is personal or commercial private information acquired by the confidant in circumstances importing an obligation of banking confidence.[142] Confider may be a real or legal person.

---

[134] ATF 64 (1938) II 162
[135] H R Steiner, M D Pfenninger, 'Bank Confidentiality in Switzerland' (1998) 1 JIBFL 14, 15.
[136] Swiss Code of Obligations, Article 396(1)
[137] Swiss Code of Obligations, Article 398(2)
[138] ATF 128 II 211, considerants 2.3 – 2.7. See also Bollmann and Gmuer (n.119), 665.
[139] Dunant and Wassmer (n,119) 543 and Chaudet (n,119), 20 ; and Guex (n,119), 5.
[140] "[…..]For the duration of the employment relationship the employee must not exploit or reveal confidential information obtained while in the employer's service, such as manufacturing or trade secrets; he remains bound by such duty of confidentiality even after the end of the employment relationship to the extent required to safeguard the employer's legitimate interests."
[141] Dunant and Wassmer (n,119), 543 ; and Chaudet (n,119), 20 ; and Sébastien Guex (n,119), Varia. 5.
[142] See 3.III.B. above.

Data may be qualified as confidential information within banking context under two conditions: it must have the necessary quality of confidence about it (material condition) and it must be obtained or observed by the banker in circumstances importing an obligation of banking confidence (cognitive condition).

There are four categories of secrets which deserve legal protection: (1) commercial secrets, (2) personal confidences, (3) artistic and literary confidences and (4) government secrets.[143] The law relating to breach of banking confidence focuses on the first two (ie. commercial secrets and personal confidences), as the rest are not related to the duty of secrecy bankers owe their clients. Therefore, the law relating to breach of banking confidence protects personal confidences and commercial secrets. The former is the one on which this thesis focuses.

3.III.B.2.a. Material condition - data having the necessary quality of confidence about it

3.III.B.2.a.i. Material condition in common law

Data may be of confidential nature if it is private in the sense that it is non-public. In *Saltman Engineering Co. Ltd v. Campbell Engineering Co. Ltd*, the Court observed that: "[t]he information, to be confidential, must have the necessary quality of confidence about it, namely, it must not be something which is public property and public knowledge".[144] Lord Goff of Chieveley, in *Attorney General v Guardian Newspapers (No 2)*, explained that

> "once it (information) has entered what is usually called the public domain (which means no more than that the information in question is so generally accessible that, in all the circumstances, it cannot be regarded as confidential) then, as a general rule, the principle of confidentiality can have no application to it." [145]

John Hull affirms that "put simply; it is secret information that have the necessary quality of confidence which is protected by the law relating to breach of confidence"[146]. Indeed, in *Elli Christofi v Barclays Bank Plc*, the Court of Appeal dismissed the appeal because the information disclosed by the confidant bank "was not secret information giving rise to a duty of confidentiality".[147]

Hull brightly established that

> The information is analogous to a freely available mineral which has to be mined to bring it to the surface, a process requiring skill, effort and sometimes money to achieve. The fact that it is not immediately accessible means that, whilst being available for those who care

[143] F Gurry, *Breach of Confidence* (OUP 1998), 82.
[144] *Saltman Engineering Co. Ltd v. Campbell Engineering Co. Ltd* (1948) 65 R.P.C. 203
[145] *Attrorney-General v. Guardian Newspapers Ltd (No. 2)* [1990] 1 AC 109, 281
[146] J Hull, *Commercial Secrecy: Law and Practice* (Sweet & Maxwell 1998), 45.
[147] [2000] 1 W.L.R. 937 1

to look, or who have the resources to obtain it, the information is not properly in the public domain.[148]

Indeed, according to Dame Elizabeth Butler-Sloss "the existence of information which can be accessed but is unlikely to be known to be available to the general public, not engaged in statistics or research of some sort, [does not] amount to being as a matter of reality in the public domain".[149] Hence, privacy of information is "a question of degree".[150] Determining whether the information is public or private, the courts consider many factors such as the number of people who hold that information or, the level of difficulty a member of the public would have in acquiring that information.[151]

3.III.B.2.a.*ii*. Material condition in Swiss federal law

Confidential data has no statutory definition in Swiss federal law. Article 28(1) of the Civil Code 1907 and articles 394-398 of the Code of Obligations 1911 are not specific to bankers' duty of secrecy. Therefore, Swiss authors define bankers' duty of secrecy with reference to Article 47 of the Banking Act 1934.[152] Accordingly, confidential data is defined as "secret information".[153] If banker reveals directly or indirectly information that is not public knowledge which the banker obtained or observed thanks to its professional relationship with its client, the banker breaches its duty of secrecy. Secrecy of information is seen as a question of degree in Swiss literature.[154] "Even information that is publicly known is protected by the banking secrecy if its disclosure by the bank gives reason to believe that a certain client has a business relationship with a certain bank".[155]

It is worth mentioning that confidential information within the banking context has been defined more restrictively in some civil law systems. For instance, French scholars Ripert and Roblot argued that "[c]onfidential information is that which shows a precise nature, notably by figures which accompany

---

[148] Hull (n,146), 55.
[149] *Attorney General v Greater Manchester Newspapers Ltd* [2001] TLR 688 at [27]
[150] Franchi v. Franchi [1967] R.P.C. 149
[151] see *Prince Albert v Strange* (1849) 41 ER 1171, *Douglas v Hello! Ltd* [2001] 2 All ER 289 at [165]; and *R v Galvin* [1987] 2 All ER 851, 856.
[152] See Bollmann and Gmuer (n.119), 665; Grassi and Calvarese (n.119), 333 ; Naim (119), 231 ; Dunant and Wassmer (n,119) 543; Chaudet (n,119), 20 Sébastien Guex (n,119), Varia. 5
[153] KPMG's unofficial translation of the Swiss Federal Act on Banks and Savings Banks, https://assets.kpmg/content/dam/kpmg/ch/pdf/ch-banking-act-en.pdf, translated the words *"un secret"* and *"Geheimnis"* used in original French and German texts respectively as "confidential information". However, secret information suits better for translating the words *"un secret"* and *"Geheimnis"*. Bollmann and Gmuer (n.119), 662. and Grassi and Calvarese in Grassi and Calvarese (n.119), 331 also preferred secret term.
[154] J L Capdeville, *Le secret bancaire: Approches nationale et internationale* (Revue Banque Édition 2014), 35; Chaudet (n,119), 20 .
[155] S Lembo and C Hensler, 'Whistleblowers in the Swiss Banking Sector: Legal Hurdles to Cooperating with Foreign Governments' (Bär & Karrer Briefing, January 2015) <https://www.baerkarrer.ch/publications/BK%20Briefing_Whistleblowers%20in%20the%20CH%20Banking%20Sector.pdf> 10 June 2021.

them: contents of balance sheet, movement of accounts. Conversely, the disclosure of general information, notably on the solvency of a person, does not conflict with secrecy."[156] Similarly, Capdeville defends that a client's general financial information disclosed by a credit institution, such as irregular payment and unpaid cheques, may not be accepted precise enough for the purposes of bank secrecy rules.[157] As both Ripert/Roblot and Capdeville accepted in 1988 and in 2014 respectively, there is not enough jurisprudential evidence on this question. Banks are strongly attached to their duty of confidentiality and do not disclose even imprecise information without using appropriate legal practices such as ethical walls.[158] Capdeville admits that this restrictive definition of confidential information has found no support in Swiss literature.[159] Cranston affirms that "in English law there is no reason to think that [precise data] is any more likely to have a confidential quality or not be common knowledge".[160]

3.III.B.2.b. Cognitive condition - acquired in circumstances importing an obligation of banking confidence.

Banks owe a duty of professional confidentiality when they obtain secret information in circumstances importing an obligation of banking confidence. The circumstances import an obligation of banking confidence when there is a relationship of confidence between the banker and its' counter-party (1) and the confidant obtained non-public information due to this relationship (2).

Accordingly, two questions arise:
1. What relations constitute a relationship of confidence which imports a duty of bank confidentiality? (Cognitive condition-1)
2. What are the circumstances in which the confidant obtains data due to this relationship? (Cognitive condition-2)

3.III.B.2.b.i. What relations constitute a relationship of confidence which imports a duty of bank confidentiality?

Banks have become multifunctional institutions engaging with "a wide range of business activity beyond their traditional core activities of deposit-taking, lending and providing payment services in

[156] Ripert et Roblot, Traité de droit commercial t. II 11th edition n 2282 via O Lajoix and M B Berlioz, 'France' in D Campbell (ed), *International Bank Secrecy* (Sweet & Maxwell 1992), 193.
[157] Capdeville (n,154), 36.
[158] See CA Paris, 6 févr. 1975, O. 1975, p. 318, note J. Vezian ; Capdeville (n,154), 36.
[159] J L Capdeville, *Le secret bancaire : étude de droit comparé (France, Suisse, Luxembourg) Tome 2* (PU Aix-Marseille 2006), 134.
[160] Cranston (n,125), 173.

connection with the operation of current accounts".[161] In English and Swiss laws, bankers owe a duty of confidentiality when they provide any financial service. In both English and Swiss laws, banks' contractual duty of confidentiality applies to their contractual relations with their clients and non-client users. Bankers tortious duty of secrecy in Swiss law and bankers' equitable duty of secrecy in English law extends to their non-contractual relations.[162]

It is possible to see more restrictive definitions in different legal systems.[163] For instance, before the Gramm-Leach-Bliley Act,[164] New York courts had recognized a duty of confidentiality between banks and their depositors due to quasi-fiduciary relationship between a bank and its depositors, yet refused to extend the duty to a borrowing relationship.[165] This has not found any support in English law.

3.III.B.2.b.ii. Circumstances in which the information may be accepted as acquired due to this relationship

As argued before, the privacy of information is a question of degree.[166] As explained in *Attorney General v Greater Manchester Newspapers Ltd*, "the existence of information which can be accessed but is unlikely to be known to be available to the general public, not engaged in statistics or research of some sort, [does not] amount to being as a matter of reality in the public domain".[167] Therefore, bankers can obtain private (ie. non-public) information in two ways. First, they can obtain such data within their professional capacity (eg. data may be disclosed to the bank by a customer or by a third party on behalf of the customer, the bank may observe data through keeping of the client's account, the bank may obtain information from public authorities in their professional capacity). Second, they can obtain such data without using their professional capacity. For instance, they can obtain information from open sources[168] or obtain information before or after their professional relationship with the client.

---

[161] E P Ellinger, E Lomnicka and C V M Hare, *Ellinger's modern banking law* (OUP 2011), 80.
[162] Ellinger et al. (n,161), 83.
[163] D Newcomb, B Burke and S Favretto 'USA' in G Godfrey and F Neate (eds), *Neate and Godfrey: Bank Confidentiality* (Bloomsbury Professional 2015), 960.
[164] The Gramm-Leach-Bliley Act 1999, Pub L No 106-102, 106th Congress, 1st Sess (12 November 1999) 113 Stat 1338 -1481 (1999). The Gramm-Leach-Bliley Act is "the first US federal statute that deals with the disclosure of non-public personal information of private individual consumers". For further information, see Danforth Newcomb et al. (n,163), 965.
[165] Young v Chemical Bank, NY LJ, Aug 7, 1992 at 21 (NY Sup Ct Aug 7, 1992); and Graney development Corp v Taksen 92 Misc 2d 764 (NY Sup Ct 1978)
[166] Franchi v. Franchi [1967] R.P.C. 149
[167] *Attorney General v Greater Manchester Newspapers Ltd* [2001] TLR 688 at [27]
[168] According to the EUROPOL's From Suspicion to Action report, open source indications and information are behind 2% of STR reporting. However, open source information may also be used while detecting other reasons. Europol Report, 'From suspicion to action: Converting financial intelligence into greater operational impact' (2017), 22 <https://www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact> 1 June 2021.

Atkin LJ in Tournier observed that banks' duty of confidentiality encompasses information concerning its customer and his affairs, "if the occasion upon which the information was obtained arose out of the banking relations of the bank and its customers".[169] Similarly, according to Bankes LJ, banks' duty of confidentiality "extents to any information, regardless of its source, acquired in the character of banker."[170] Although Scrutton LJ disagreed with this view arguing "that the implied legal duty towards the customer to keep secret his affairs does not apply [….] to knowledge derived from other sources during the continuance of the relation",[171] the courts have subsequently preferred the majority view.[172]

Swiss Banking Act Article 47 applies to the bankers to whom secret information is "entrusted […] in their capacity as a member of an executive or supervisory body, employee, representative or liquidator of a bank, as member of a body or employee of an audit firm or that they have observed in this capacity". Similarly, in Swiss private law, information may be confidential if the bank has acquired it in its' professional capacity.[173]

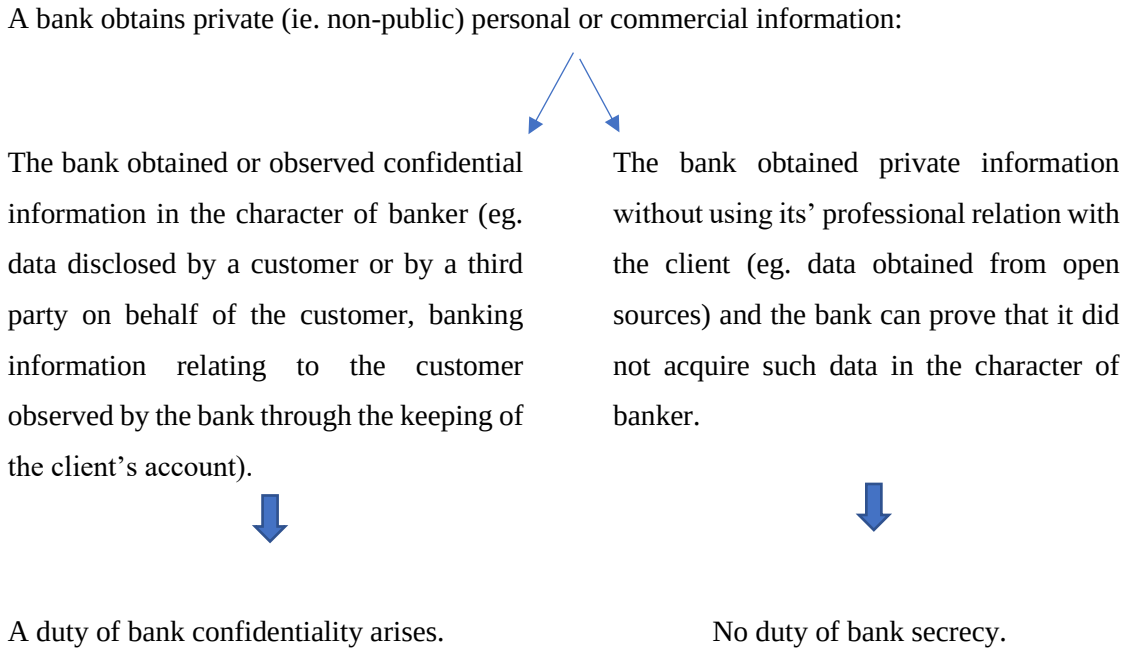
Where a bank acquired private data without using its' professional capacity, a duty of confidentiality does not arise. For instance, data obtained by the bank before or after its' professional relationship with its' client cannot be qualified as confidential data.[174]

To protect banking clients' privacy and confidentiality rights effectively, any private data of the client legitimately acquired by the bank within the course of their professional relationship is presumed to have been obtained by the bank in the character of banker. The bank shoulders the burden of proving that it did not obtain private data in the character of banker.[175] The bank can prove this by using ethical walls, also known as Chinese wall. "In finance, a Chinese Wall … is a virtual information barrier erected between those who have material, non-public information and those who do not, to prevent conflicts of interest".[176] As ethical walls impede the exchange of confidential data between different parts of the bank, one department of the bank may owe duty of confidentiality while another does not.

Some departments of a bank are typically above the wall (eg Legal, Compliance and Risk Management unit, who are also in charge of bank's AML/CTF policies, as well as Internal Audit and Corporate Security units). "Persons who are above the wall may have access to material non-public information

[169] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B. 461 , 485
[170] Ibid.
[171] Ibid, 481
[172] For instance, *Barclays Bank Plc v Taylor* [1989] 1 WLR 1066, Lipkin Gorman v. Kapnale Ltd [1989] 1 WLR 1340.
[173] Bollmann and Gmuer (n.119), 663. and S S Breitenstein, 'Switzerland' in G Godfrey and F Neate (eds), *Neate and Godfrey: Bank Confidentiality* (Bloomsbury Professional 2015), 921.
[174] Capdeville (n,154), 28.
[175] C F Green, 'Business ethics in banking' (1989) 8 *Journal of Business Ethics* 631, 633.
[176] 'Chinese wall', Corporate finance Institute website, <https://corporatefinanceinstitute.com/resources/knowledge/finance/chinese-wall-definition/> 10 June 2021.

on both sides of the information barriers." [177] If data is qualified as confidential data on, at least, one side of the wall, it constitutes confidential data for persons and teams above the wall.



3.III.B.2.c. A duty that may be qualified or limited

While some offshore countries accept strict secrecy terms, bankers' legal duty of secrecy in English and Swiss laws has never been unimpeachable. Bankers' duty of confidentiality could and can still be qualified or limited for some pressing social needs, one of which is the prevention and prosecution of crime. Therefore, bankers' legal duty of secrecy does not require them to keep their mouth shut concerning their clients' criminal activities.

Bankes LJ in *Tournier* put it that bankers' duty of confidentiality is not absolute but qualified.[178] There are four heads of qualifications, two of which are as follows: [179] Where disclosure is under compulsion by law (eg. "duty to obey an order under the Bankers' Books Evidence Act",[180] disclosure of suspicion or information about a crime already committed[181]) and where there is a duty to the public to disclose

[177] Ibid.
[178] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B. 461, at 472-473 (by Bankes LJ)
[179] Ibid. Third and fourth heads of qualifications to the duty of confidentiality are formulated by Bankes LJ as follows: where the interests of the bank require disclosure, and where the disclosure is made by the express or implied consent of the customer. These heads of qualifications will not be further investigated in this chapter as they do not apply to the banks making SARs to comply with their duty of reporting.
[180] Ibid. For further examples see Aplin et al (n,131), 9.53.
[181] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B. 461, at 471; Price Waterhouse v BCCI [1992] BCLC 583, 598 (by Millet J.); Aplin et al.(n,131), 9.53.

("cases where a higher duty than the private duty is involved, such as where "danger to the State or public duty may supersede the duty of the agent to his principal"[182]). Similarly, it was recognised in *Attrorney-General v. Guardian Newspapers Ltd* that public interest in the protection of an equitable duty of confidentiality "may be outweighed by some other countervailing public interest which favours disclosure".[183]

As previously explained, bankers' duty of confidentiality in Swiss federal law finds its legal basis in contract, tort and criminal laws. Article 47 of the Swiss Banking Act does not create an absolute duty of secrecy. Its paragraph 5 stipulates that "The federal and cantonal provisions on the duty to provide evidence or on the duty to provide information to an authority shall be exempted from this provision".[184] Neither does article 28 of the Code Civil lead an unimpeachable duty of secrecy. According to its' second paragraph, one's personality rights can lawfully be interfered with if "it is justified by the consent of the person whose rights are infringed or by an overriding private or public interest or by law." Lastly, bankers' contractual duty of secrecy is limited with the principle of *Conventio privatorum non potest publico juri derogare*.[185] Hence, Swiss banking secrecy concept has limits under civil law (eg. regulations on inheritance and powers of attorney) and public law (eg. criminal and civil procedure provisions, tax regulations and Anti-Money-Laundering and counter-terrorist financing legislation) which are justified by the prevailing public interest.[186] Hence, banks' duty of secrecy may be limited for the detection, prevention and prosecution of crime.

Article 13(1) of the Federal Constitution of the Swiss Confederation recognises everyone's right to privacy. Article 35 of the Federal Constitution recognises vertical and horizontal applicability of fundamental rights. Right to privacy encompasses banking clients' right to professional secrecy.[187] According to article 36 of the Federal Constitution,

> 1 Restrictions on fundamental rights must have a legal basis. …
>
> 2 Restrictions on fundamental rights must be justified in the public interest or for the protection of the fundamental rights of others.
>
> 3 Any restrictions on fundamental rights must be proportionate.
>
> 4 The essence of fundamental rights is sacrosanct.

---

[182] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B. 461, at 473 (by Bankes LJ); see also *Weld-Blundell* v. *Stephens* [1920] A. C. 956, 965.
[183] Attrorney-General v. Guardian Newspapers Ltd (No. 2) [1990] 1 AC 109, 281
[184] Unofficial translation of Swiss Federal Act on Banks and Savings Banks dated 8 November 1934 (version as at 1 January 2019), translated by KPMG. Available at: https://assets.kpmg/content/dam/kpmg/ch/pdf/ch-banking-act-en.pdf
[185] ATF 131 III 217, cons. 4. See also N Rouiller, *Droit suisse des obligations et Principes du droit européen des contrats* (Cedidac 2007), 86.
[186] Grassi and Calvarese (n.119), 329.
[187] ATF 82 II 555 consid. 7; ATF 133 III 664 consid. 2.5.

Hence, AML laws that permit and require banks to produce SARs must be justified in the public interest or for the protection of the fundamental rights of others, must be proportionate and must not touch upon the essence of the right to privacy.

As will be explained in the following part, the extent to which banks' duty of secrecy can be limited is influenced by Article 8 of ECHR too.

3.III.B.3. Conclusion

The law of confidence has long but partially protected banking clients' control rights over their personal data. Law of confidence permits interference with banking clients' right to professional confidentiality under certain conditions. For instance, banks are permitted to share confidential information with a public authority where the law requires them to do so.

3.III.C. Bankers' information privacy rights and the European Convention on Human Rights

English and Swiss laws should respect the ECHR, and Article 8 of the Convention applies to the SARs regime related cases. Therefore, English and Swiss AML laws relating to the STRs regime should respect Article 8 of the ECHR.

3.III.C.1. The SARs produced by banks and Article 8 of the ECHR

Article 8 of the ECHR recognises everyone's "right to respect for his private and family life, his home and his correspondence". Banking information within an STR may fall under the notion of "private life" and/or "correspondence", and the disclosure of such information to a public authority by the reporting bank may amount to interference for the purposes of Article 8. In *Sommer v Germany*, the Court established that[188]

> collecting, storing and making available the applicant's professional bank transactions constituted an interference with his right to respect for professional confidentiality and his private life.

"Information retrieved from banking documents undoubtedly amounts to personal data concerning an individual, irrespective of it being sensitive information or not".[189] An STR is a report by which the

[188] *Sommer v Germany* (2018) 67 E.H.R.R. 9, [48]; see also *M.N. and others v San Marino* (2016) 62 E.H.R.R. 19, [51]–[55]; *Brito Ferrinho Bexiga Villa-Nova v Portugal* (69436/10) (Unreported, December 1, 2015) (ECHR), [44]; and *Michaud v France* (2014) 59 E.H.R.R. 9, [90]–[92].
[189] *M.N. and others v San Marino* (2016) 62 E.H.R.R. 19, [51].

reporting person informs the FIU that it knows or suspects that its' client's funds constitute or represent proceeds of crime. Accordingly, an SAR filed by a bank relating to an individual banking client involve personal information. Processing or use of personal data may be of a nature to constitute an interference with respect for private life.[190] The ECtHR established that both the storing and the release of information relating to an individual's private life falls within the application of Article 8-1.[191] The Court interpretes the 'private life' largely and established that there is no reason of principle to justify excluding information relating to one's professional and business life from the notion of private life.[192] In *Amann v Switzerland*, the Court commented on the 'private life' as follows:[193]

> [T]he term "private life" must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings; furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life" (see the Niemietz v. Germany judgment of 16 December 1992, Series A no. 251-B, pp. 33-34, § 29, and the Halford judgment cited above, pp. 1015-16, § 42).
>
> That broad interpretation corresponds with that of the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose purpose is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined as "any information relating to an identified or identifiable individual" (Article 2).

In *Rotaru v Romania*, the Court emphasised that "public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities."[194]

Hence, Article 8 is applicable to the disclosure of STRs related cases.

---

[190] *Uzun v Germany* (2011) 53 E.H.R.R. 24, [47]; *Perry v the United Kingdom* (2004) 39 E.H.R.R. 3, [40]–[41].
[191] *Leander v Sweden* (1987) 9 E.H.R.R. 433, [48].
[192] *M.N. and others v San Marino* (2016) 62 E.H.R.R. 19, [51]; *Amann v. Switzerland* (2000) 30 E.H.R.R. 843, [65].
[193] *Amann v. Switzerland* (2000) 30 E.H.R.R. 843, [65].
[194] *Rotaru v Romania* [2000] 5 WLUK 77, [43]. In *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, the ECtHR Grand Camber established that (*Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* (2018) 66 E.H.R.R. 8, [137].)

> The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article (see *S. and Marper*, cited above, § 103). Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged.

The state imposes upon banks duty to make STRs. Moreover, it is a state authority, the FIU, that receives the STRs. Requiring and permitting banks to make STRs also means permitting the FIU to receive STRs. While the reporting bank has some discretionary power, the STRs regime related cases are related to the state's negative obligation to abstain from arbitrary interference.[195] The Court described the state's negative obligation as the essential object of Article 8.[196]

The ECtHR indicates that the contracting parties have also positive obligations involving "the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves" in addition to their duty to abstain from arbitrary interference.[197] In the Court's view, "a complaint under Article 13 as to the absence of an effective domestic remedy is subsidiary to the complaint under Article 8 of the Convention that the State did not ensure respect for the private life".[198] Therefore, domestic law should take measures to ensure respect for private life.[199]

Interference with one's exercise of his/her Article 8-1 rights "breaches Article 8 unless it is "in accordance with the law", pursues one or more of the legitimate aims referred to in paragraph 2 and, in addition, is "necessary in a democratic society" to achieve those aims."[200].

First of all, the interference should be "in accordance with the law". The concept of law covers common law provisions too.[201] The law must be clear, foreseeable, and accessible.[202] The law must be sufficiently clear and foreseeable in its terms to give individuals an adequate indication as to the circumstances in which their bankers can share their banking data with the law enforcement agencies.[203] However, foreseeability need not be certain, the applicants should be able to foresee to a reasonable degree, at least with the advice of the experts.[204]

---

[195] Libert v France, App no 588/13, Fifth Chamber of the European Court of Human Rights, 22 February 2018, [40]-[42]

[196] *Kroon v. the Netherlands* (1995) 19 E.H.R.R. 263, [31].

[197] *I v Finland* (2009) 48 E.H.R.R. 31 at [36]. "Article 8 protects the confidentiality of all the exchanges in which individuals may engage for the purposes of communication," (*M.N. and others v San Marino* (2016) 62 E.H.R.R. 19, [52]; *Michaud v France* (2014) 59 E.H.R.R 9 at [90].) and the disclosure of confidential information by the confidant to a third party constitutes an interference with respect for correspondence. (*I v Finland* (2009) 48 E.H.R.R. 31, [36]; *Armoniene v Lithuania* (2009) 48 E.H.R.R. 53, [23]. For further analysis, see O Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015) 113-118.) The SARs produced by banks involve confidential information. Accordingly, AML laws that require and/or permit the confidant bank to file SARs with the Financial Intelligence Units interfere with banking clients' Article 8 rights. (See *Michaud v France* (2014) 59 E.H.R.R 9 at [121] relating to the lawyers' duty to produce SARs.) Therefore, such laws must be in compliance with Article 8-2 of the Convention.

[198] *Armoniene v Lithuania* (2009) 48 E.H.R.R. 53 at [23].

[199] *Evans v. the United Kingdom* (2008) 46 E.H.R.R. 34, [75]

[200] *Amann v. Switzerland* (2000) 30 E.H.R.R. 843, [71].

[201] Kruslin v. France [1990] 4 WLUK 184, [29]

[202] *Silver v. the United Kingdom*, (1981) 3 E.H.R.R. 475, [87]

[203] Fernandez Martinez v Spain (2015) 60 E.H.R.R. 3, [117]; and Shimovolos v. Russia, (2014) 58 E.H.R.R. 26, [68]

[204] Dubská and Krejzová v. the Czech Republic (2017) 65 E.H.R.R. 5, [171] and Slivenko v. Latvia (2004) 39 E.H.R.R. 24, [41].

One of the legitimate purposes referred to in Article 8-2 is "the prevention of disorder or crime". An interference is "necessary in a democratic society" to achieve one or more of the legitimate aims if it is necessary and proportionate to achieve those aims.[205] "When considering the necessity of interference, the Court must be satisfied that there existed sufficient and adequate guarantees against arbitrariness, including the possibility of an effective control of the measure at issue".[206]

In the proportionality test, the Court takes into account the level of risk to one's rights and freedoms caused by the loss of confidentiality of data protected by professional secrecy. The level of risk to rights and freedoms depends on the nature of the information protected and the nature of the relationship of confidence. Therefore, the extent to which Article 8 permits interference with the right to professional secrecy depends on the nature of confidential information and the relationship of confidence. Considering these two factors, Article 8 affords strengthened protection to exchanges between lawyers and their clients[207] and doctors and patients.[208]

To understand the risk to clients' rights and freedoms by the loss of confidentiality of data protected by bank secrecy, it is necessary to consider the nature of the confidential information (banking data) and the relationship of confidence (banking relation) at stake. It is worth mentioning that unauthorised disclosure of banking data can give rise to financial loss and damage to the reputation of the data subject.

---

[205] *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* (2018) 66 E.H.R.R. 8, [164]; Z v Finland (1998) 25 E.H.R.R. 371 at [94]; *Cremieux v France* (1993) 16 E.H.R.R. 357, [38]; *Klass and Others* ***v****. Germany (A/28):* (1978) 2 E.H.R.R. 214, [42].

[206] *M.N. v San Marino* (2016) 62 E.H.R.R. 19 at [73]. See also *Matheron v France* (57752/00) (Unreported, March 29, 2005) (ECHR), [35]; *Lambert v France* (2000) 30 E.H.R.R. 346, [49]; *Xavier Da Silveira v. France* (43757/05) (Unreported, January 21, 2010) (ECHR), [43] and *Klass and Others* ***v****. Germany (A/28):* (1978) 2 E.H.R.R. 214, [54], [55].

[207] The Court affirmed, in *Michaud v France* (2014) 59 E.H.R.R 9, [118], that

> "[…] while Article 8 protects the confidentiality of all "correspondence" between individuals, it affords strengthened protection to exchanges between lawyers and their clients. This is justified by the fact that lawyers are assigned a fundamental role in a democratic society, that of defending litigants."

See also *Wieser and Bicos Beteiligungen GmbH v Austria* (2008) 46 E.H.R.R. 54 at [65] and [66], *Niemietz v Germany* (1993) 16 E.H.R.R. 97 at [37], *André and Another v. France* (24 July 2008)18603/03 at [41].

[208] The ECtHR recognised a special place for medical and legal confidentiality. In *Z v Finland* (1998) 25 E.H.R.R. 371, [96], the Court affirmed that

> in view of the highly intimate and sensitive nature of information concerning a person's HIV status, any State measures compelling communication or disclosure of such information without the consent of the patient call for the most careful scrutiny on the part of the Court, as do the safeguards designed to secure an effective protection.

Moreover, the Court stressed out that

> respecting the confidentiality of health data [….] is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession.[…] The interests in protecting the confidentiality of such information will therefore weigh heavily in the balance in determining whether the interference was proportionate […].

Judge De Meyer had gone further in his partly dissenting opinion in the same case affirming that "[…]whatever the requirements of criminal proceedings may be, considerations of that order do not justify disclosing confidential information arising out of the doctor/patient relationship or the documents relating to it." (Z v Finland (1998) 25 E.H.R.R. 371 at page 34) See also Dudgeon v. the United Kingdom (1983) 5 E.H.R.R. 573 at [21] and [52], Johansen v. Norway (1997) 23 E.H.R.R. 33 at [64].

3.III.C.2. The ECHR's place in English and Swiss laws

The ECHR affects both English and Swiss laws. Swiss law should comply with the ECHR, because the convention rights arguably have a supra-constitutional value in Switzerland. Moreover, the rights and freedoms of individuals set forth in Section I of the ECHR have a privileged status compared to other laws in the English legal system.

3.III.C.2.a Swiss federal law and the Convention rights as interpreted by the ECtHR

Bankers' duty and/or right to produce SARs are determined in SCC 1937 and AMLA 1997, both of which are federal acts. The courts should interpret federal acts in compliance with the ECtHR's article 8 jurisprudence. Moreover, the courts should apply Article 8 of the ECHR where AML laws that permit and/or require banks to produce SARs conflicts with Article 8 of ECHR.

Switzerland signed and ratified the ECHR in 1974 with two reservations and two interpretative declarations.[209] Yet, none of these reservations and declarations is in force today.[210] Because Switzerland is a monist jurisdiction, [211] the ECHR constitutes an integral part of Swiss Federal law. Because article 32 of the ECHR is also an integral part of Swiss federal law, the ECtHR's jurisdiction extends "to all matters concerning the interpretation and application of the Convention and the Protocols thereto which are referred to it as provided in Articles 33, 34, 46 and 47".

In the Federal Supreme Court's jurisprudence, administrative authorities, as well as courts, shall directly apply a provision of international law under three cumulative conditions: (i) the provision concerns the rights and obligations of the individual, (ii) the provision is justiciable, that is to say sufficiently concrete and clear to be directly applicable to a specific case by an authority or a court and (iii) the provision is addressed to authorities responsible for applying the law and not to legislative authorities only.[212]

---

[209] Federal Decree on the acceptance of the ratification of the ECHR, 3 October 1974, AS 1974 2148, BBI 1974 I 1068. For further details in relation to Switzerland's acceptance and ratification of the ECHR and its' additional protocols, see A Haefliger, «Le Tribunal Fédéral Suisse » in Annuaire international de justice constitutionnelle – La hiérarchie des normes constitutionnelles et sa fonction dans la protection des droits fondamentaux, Le principe de non-rétroactivité des lois 1990, 6, 195, 195-196. <https://www.persee.fr/doc/aijc_0995-3817_1992_num_6_1990_1131> 10 June 2021.

[210] For further details, see D Thurnherr 'The reception process in Austria and Switzerland' in H Keller and AS Sweet (eds), *A Europe of Rights: The Impact of the ECHR on National Legal Systems* (OUP 2008), 316-318.

[211] Switzerland's monist character is reflected in its' Federal Constitution. First, all public authorities in the Confederation and the Cantons are under a constitutional duty to respect international law (Article 5(4) of the Federal Constitution of the Swiss Confederation.). Moreover, judicial authorities are given a constitutional duty to apply federal acts and international law (Article 190 of the Federal Constitution of the Swiss Confederation.) Accordingly, signed and ratified international treaties are incorporated eo ipso into Swiss federal law. .

[212] ATF 136 I 297 E. 8.1 and ATF 133 I 286 E. 3.2. In relation to direct applicability of international treaties, see L Caflisch, « La pratique suisse en matière de droit international public » Département fédéral des affaires

According to the Federal Supreme Court's consistent jurisprudence, rights and freedoms set forth in Section I of the Convention meet all three conditions and, therefore, are directly applicable.[213] Hence, not only legislator but also administrative authorities and courts are automatically required to apply Section I of the Convention.

Both cantonal and federal laws (eg. SCC 1937 and AMLA 1997) should be in compliance with the rights enshrined in Section I of the ECHR. The Federal Supreme Court is required to interpret federal and cantonal law in compliance with the Convention. Courts must apply the Convention rights where a convention right as interpreted by the ECtHR and a federal act conflict.

All acts of administrative authorities, including regulations adopted by them, must be "based on and limited by law"[214] and international law is an integral part of national law. An administrative act that is in breach of a directly applicable provision of international law can only be valid if it is adopted on the basis of another piece of law that overrides relevant international law provision.[215] Similarly, courts can apply a piece of law that is in breach of a directly applicable provision of international law if and only if the former takes precedence over the latter.[216] However, it is worth mentioning that all public authorities are under a duty to interpret domestic law in compliance with international law as far as possible.[217] The Federal Supreme Court finds the basis of this duty in articles 5(4) and 5(3) of the Federal Constitution. Accordingly, interpretation of public authorities' duty to respect international law[218] in good faith[219] requires them to interpret domestic law in compliance with international law as far as possible. Consistent interpretation is not aimed at resolving conflicts between domestic law and international law, but rather at preventing such conflicts.[220] Indeed, as long as domestic law can be interpreted in accordance with international law, no conflict arises.[221] Because the ECHR is a directly

étrangères, 2013, 6, <https://www.eda.admin.ch/dam/eda/fr/documents/das-eda/organisation-eda/130425-RSDIE-pratique-2011-complet_fr.pdf> 6 June 2021; M. Hottelier, « Le contrôle de constitutionnalité des décisions de justice en Suisse ou l'exercice d'un contrôle concret des normes » 114, <https://dice.univ-amu.fr/sites/dice.univ-amu.fr/files/public/122-hottelier.pdf> 6 June 2021.

[213] ATF 126 II 324, 327. In relation to direct applicability of the Convention, see G Kolly, « Le Tribunal fédéral Suisse », in the Tribunal Federal's webpage, 4-5, <https://www.bger.ch/files/live/sites/bger/files/pdf/de/cahiers-cc_201606.pdf> 10 June 2021; and Haefliger (n,209), 208.

[214] Article 5(1) of the Federal Constitution of the Swiss Confederation.

[215] [ATF] 99 Ib 39. For further information in relation to judicial control of administrative authorities' compliance with directly applicable provisions of international law, see A Jomini, « Présentation du Tribunal fédéral suisse comme autorité de juridiction constitutionnelle » Cahiers du Conseil Constitutionnel n° 18 (Dossier : Suisse) - Juillet 2005, 3-6, <https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/presentation-du-tribunal-federal-suisse-comme-autorite-de-juridiction-constitutionnelle> 10 June 2021.; Hottelier (n,212), [3.1.2] and [3.1.3.].

[216] [ATF] 99 Ib 39 and [ATF] 112 II 1.

[217]ATF 117 Ib 367, 373; ATF 94 I 669; ATF 106 Ia 406; ATF 106 Ia 180 . See also FF 2010 2067 « La relation entre droit international et droit interne » in Rapport du Conseil fédéral, 5 March 2010, 2018, <https://www.admin.ch/opc/fr/federal-gazette/2010/index_13.html> 10 June 2021.

[218] Article 5(4) of the Federal Constitution of the Swiss Confederation.

[219] Article 5(3) of the Federal Constitution of the Swiss Confederation provides that "[s]tate institutions … shall act in good faith".

[220] FF 2010 2067, (n,217), 2108.

[221] Ibid.

applicable piece of international law, all public authorities are under duty to interpret and apply domestic law in compliance with the Convention as far as possible.

Swiss legal order adheres to the monist principle that international law takes precedence over national law.[222] However, international law's supremacy is not absolute. The Federal Supreme Court accepts that there are exceptions to the primacy of international law.[223]

Convention rights are of supreme legal value in Switzerland, the only jurisdiction where the Convention is arguably of a supra-constitutional value.[224] Moreover, the judiciary plays an important role in supervising this supremacy. The Convention's place in the hierarchy of norms may be explained in four steps: the relationship between the ECHR, on the one hand, and (i) cantonal acts, (ii) cantonal constitutions, (iii) federal acts and other international treaties and (iv) the Federal constitution, on the other hand.

3.III.C.2.a.i. ECHR vs cantonal legislation

The ECHR takes precedence over cantonal acts. Moreover, the duty of supervising cantonal acts' compliance with the Convention is given to the judiciary.

Article 190 of the Federal Constitution of the Swiss Confederation provides that "the Federal Supreme Court and the other judicial authorities apply the federal acts and international law". The Federal Supreme Court interprets this norm as meaning that international law constitutes *lex superior* to all domestic norms except federal acts.[225] Accordingly, cantonal acts ought to comply with the ECHR, an international treaty signed and ratified by Switzerland.

Judiciary is given the task to supervise the compliance of cantonal acts with the Convention. First, any court that is to apply cantonal law is under the duty not to apply provisions of a cantonal act that contradict international law.[226] Second, provisions of a cantonal act can be declared invalid by the

[222] ATF 125 II 417, 424 and ATF 128 IV 201, 205.
[223] See for example ATF 99 Ib 39 ; and ATF 112 II 1. For further information, see Caflisch (n,212), 6.
[224] Most members of the Council of Europe recognise the ECHR as of supra-legislative but sub-constitutional value. For a comprehensive investigation of the rung of the ECHR in hierarchy of norms in several jurisdictions, see H Keller and A S Sweet (eds), *A Europe of Rights: The Impact of the ECHR on National Legal Systems* (OUP 2008), Part II.
[225] ATF 117 Ib 367; ATF 125 II 417; ATF 118 Ib 281; ATF 119 V 171.
[226] Arrêt du Tribunal Fédéral Suisse 6B_856/2014 du 10 juillet 2015 dans la cause X. c. Ministère public de la République et canton de Genève, consid. 3.3, cited in « Chronique suisse de justice constitutionnelle 2015 », AIJC XXXI-2015, p. 900. For further details in relation to diffuse and concrete constitutionality review of statutes in Switzerland, see Hottelier (n,212), 114-121.

Federal Supreme Court or a competent cantonal court[227] if the cantonal act is in breach of international law.[228]

To summarise, rights and freedoms set forth in Section I of the ECHR supersede provisions of cantonal acts. Cantonal acts that are in breach of these rights and freedoms can be declared invalid by the competent courts.

3.III.C.2.a.ii. ECHR vs cantonal constitutions

Not only cantonal acts but also cantonal constitutions shall comply with federal laws, international law and the Federal Constitution.[229] Hence, cantonal constitutions should also comply with the Convention. What makes the cantonal constitutions different from other cantonal acts is the constitutional guarantee granted to the former by the Federal Assembly by virtue of Article 172(2) of the Federal Constitution.[230] According to Article 189(4), it is only acts of the Federal Assembly or the Federal Council that cannot be challenged before the Federal Supreme Court.[231] However, Article 172(2) of the Constitution, constitutes *lex specialis* to Article 189 (4). The Federal Supreme Court declared itself incompetent to examine the conformity of the provisions of the cantonal constitutions with the rights guaranteed by the ECHR.[232] Hence, while the cantonal constitutions should be in compliance with the Convention, their conformity with the Convention cannot be supervised by the judiciary. The Federal Supreme Court provides that examination of the conformity of the cantonal constitutions' provisions with the rights guaranteed by the ECHR is incumbent on the Federal Assembly and the latter must carry it out before granting the guarantee to the cantonal constitutions.[233] Hence, it is the Federal Assembly that should supervise the conformity of the provisions of the cantonal constitutions with the rights and freedoms guaranteed by the ECHR.[234]

[227] Some cantons established a cantonal supreme court where validity of cantonal law may be challenged. Cantonal supreme courts do not limit the Federal Supreme Court's powers. However, validity of cantonal laws can be challenged before the Federal Supreme Court once a decision on the issue by the cantonal supreme court was held.
[228] ATF 118 Ib 281; ATF 119 V 171.
[229] ATF 128 IV 201, 205-207 and Decision of 12 October 2012 (2C_828/2011) Consideration 5. For further information see Hottelier (n,212), [1.4].
[230] According to paragraphs 1 and 2 of Article 172 of the Federal Constitution, "The Federal Assembly shall ensure the maintenance of good relations between the Confederation and the Cantons. It shall guarantee the cantonal constitutions."
[231] ATF 111 Ia 239 rec. 3.
[232] ATF 111 Ia 239 rec. 3. See also, See also FF 2010 2067, (n,217), [5.1]-[5.4];
[233] ATF 111 Ia 239 rec. 3.
[234] FF 2010 2067, (n,217), 2089

3.III.C.2.a.iii. ECHR vs federal acts and other international treaties

Article 189(4) of the Federal Constitution provides that "[a]cts of the Federal Assembly or the Federal Council may not be challenged in the Federal Supreme Court". Accordingly, the Federal Supreme Court is incompetent to declare federal law invalid even where it is in breach of international law. However, if there is a conflict between a provision of federal law and international law, the Court is required to apply the latter by virtue of the principle that *lex superior derogat legi inferiori*. According to the Federal Supreme Court's interpretation, international treaties, once ratified, supersede federal legislation by virtue of Article 5(4) of the Federal Constitution.[235] However, the Court recognised an exception to the relevant supremacy of international law. In its' famous 'Jurisprudence Schubert' in 1973, the Court recognised that federal legislator can enact, with full knowledge of the facts, a domestic rule contrary to international law.[236] Therefore, the Federal Supreme Court is exceptionally bound to apply federal law in breach of international law, where the legislator was fully aware, by enacting the law, that it would be contrary to international law. As an exception to exception, the Court provides that human rights guaranteed by international law, in particular rights and freedoms recognised in section I of the ECHR, nevertheless systematically prevail over federal laws.[237] Hence, while the Court is incompetent to declare federal law invalid even when it is in breach of the Convention, it shall apply the Convention provisions instead of the federal act.

Another consequence of article 189(4) of the Federal Constitution is that signed and ratified international treaties cannot be challenged before the Federal Supreme Court.[238] Accordingly, the Court is incompetent to declare international treaties invalid even when provisions of a treaty conflicts with the ECHR, another international treaty. However, the Court recognises the primacy of human rights conventions over treaties with more special content. Accordingly, the Convention takes precedence over any and all bilateral treaties violating human rights.[239]

To summarise, the ECHR supersedes federal law and other international treaties. Yet, the powers of the judiciary in supervising the compliance of federal law provisions with the Convention is limited.

[235] ATF 125 II 417, 424; 128 IV 201, 205; and Decision of 12 October 2012 (2C_828/2011) Consideration 5.
[236] ATF 99 Ib 39 (Jurisprudence Schubert). Jurisprudence Schubert is confirmed in many cases. For instance, see ATF 111 V 203; 112 II 13; 116 IV 269; 117 Ib 369.
[237] ATF 125 II 417, 424 and ATF 128 IV 201, 205. See also Caflisch (n,212), 13. For other exceptions to Jurisprudence Schubert, see [ATF] 139 I 16; [ATF] 136 II 241 and [ATF] 122 II 234.
[238] ATF 126 II 324, 326.
[239]ATF 126 II 324, 327. See also Caflisch (n,212), 5.

3.III.C.2.a.iv. ECHR vs Federal Constitution

Articles 193(4) and 194(2) of the Federal Constitution provide that partial and total constitutional revisions must not violate the mandatory provisions of international law (*jus cogens*). In its' jurisprudence, the Federal Supreme Court recognised that certain guarantees of the ECHR involve the mandatory provisions of international law.[240] Hence, partial or total constitutional revisions must not violate guarantees of the Convention if and the extent to which the latter reflect *jus cogens*.

While certain guarantees of the Convention are protected against any violation by a partial or total constitutional revision, no provision in the Federal Constitution supports the idea that the Convention is a supra-constitutional norm *per se*. Nor did the Federal Supreme Court expressly argue so. However, in the Federal Supreme Court's jurisprudence, the Convention provisions take precedence over the Federal Constitution's provisions. According to the Federal Supreme Court, administrative authorities and courts cannot directly apply a provision of the Federal Constitution if it conflicts with the provisions of the ECHR.[241]

The Federal Supreme Court interprets article 189(4) of the Constitution as meaning that it is incompetent to declare provisions of the ECHR invalid even when they conflict with the Federal Constitution.[242] The Federal Supreme Court accepts that when there is a conflict between a provision of the ECHR and a provision of the Federal Constitution, the former should be applied if the latter is not directly applicable.[243] Courts or administrative authorities cannot directly apply a constitutional provision if it needs to be clarified by the legislator. The Federal Supreme Court decided that if a provision of the Federal Constitution conflicts with the provisions of the ECHR as interpreted by the ECtHR, the provision of the Federal Constitution cannot be directly applicable.[244] In a line of cases in 2013, the Federal Supreme Court decided that paragraphs 3 to 5 of article 121 of the Federal Constitution is not directly applicable by administration and courts. Paragraphs 3 to 5 of article 121 of the Federal Constitution were as follows:

> (3) Irrespective of their status under the law on foreign nationals, foreign nationals shall lose their right of residence and all other legal rights to remain in Switzerland if they:
> a. are convicted with legal binding effect of an offence of intentional homicide, rape or any other serious sexual offence, any other violent offence such as robbery, the offences of trafficking in human beings or in drugs, or a burglary offence; or
> b. have improperly claimed social insurance or social assistance benefits.

[240] ATF 139 I 16; ATF 136 I 87; ATF 133 I 27.
[241] ATF 139 I 16
[242] ATF 126 II 324, 326.
[243] ATF 139 I 16.
[244] ATF 139 I 16

(4) The legislature shall define the offences covered by paragraph 3 in more detail. It may add additional offences.

(5) Foreign nationals who lose their right of residence and all other legal rights to remain in Switzerland in accordance with paragraphs 3 and 4 must be deported from Switzerland by the competent authority and must be made subject to a ban on entry of from 5–15 years. In the event of reoffending, the ban on entry is for 20 years.

The Federal Supreme Court decided that the above-mentioned paragraphs 3 and 5 cannot be applied to a foreigner who has a residence permit in Switzerland and who was sentenced to 18 months' deprivation of liberty for drug trafficking. The Court did not defend that paragraphs 3 and 5 are grammatically unclear. The reason why the Court decided that these provisions cannot be directly applied in this case is that applying paragraph 3 with no further condition would constitute an unproportionate interference with the individual's Article 8 ECHR rights as interpreted by the ECtHR and that a provision of the Federal Constitution cannot be directly applicable if it is in breach of the ECHR.[245] The Court's relevant line of jurisprudence initiated a sovereignty debate, which led to a popular initiative: Federal popular initiative 'Swiss law instead of foreign judges (initiative for self-determination)'.[246] This popular initiative was rejected in 2016 by popular vote.[247]

To summarise, the ECHR is not a supra-constitutional norm in theory. Yet, it may take precedence over the provisions of the Federal Constitution in practice.

3.III.C.2.b. English law and the Convention rights and freedoms

Human Rights Act 1998 (HRA 1998) transposed the European Convention to national law, and "serves as an 'ethical compass' guiding the executive, legislative and judicial branches of .. [English] democratic system in the direction of 'Magnetic North" [248] setting "in place a scheme which preserves the distinct roles of the judges and politicians in the constitutional order of the United Kingdom".[249] While the Convention rights are given a privileged status compared to primary legislation and subordinate legislation, relevant privileges are not as strong as those in Switzerland. Moreover, the judiciary has relatively weaker powers to protect Convention rights against primary legislation and subordinate legislation.

[245] ATF 139 I 16.

[246] « Initiative populaire fédérale « Le droit suisse au lieu de juges étrangers (initiative pour l'autodétermination) »». <https://www.bk.admin.ch/ch/f/pore/vi/vis460t.html> 10 June 2021.

[247] FF 2019 5651, Arrêté du Conseil fédéral constatant le résultat de la votation populaire du 25 novembre 2018 – Article 2(2). <https://www.bk.admin.ch/ch/f/pore/vi/vis460.html> 10 June 2021.

[248] Lord Lester QC, Interview, 13 December 2011, referred in A Donald, J Gordon and P Leach, "The UK and the European Court of Human Rights" (2012) 83 Equality and Human Rights Commission Research report, 156.

[249] R White and C Ovey, *Jacobs, White and Ovey: The European Convention on Human Rights*. (5th edn, OUP 2010), 102.

The legislator's power to enact a law that is in breach of the rights and freedoms of individuals set forth in Section I of the ECHR is not taken away, but limited. Courts are required to interpret primary and subordinary legislation (eg. POCA 2002) in compliance with the Convention rights as far as possible. However, they cannot apply the Convention rights if there is an act in breach of the Convention. Administrative authorities must act in compliance with the rights and freedoms of individuals set forth in Section I of the ECHR unless primary legislation requires them to do so.

The legal value of rights and freedoms of individuals set forth in Section I of the ECHR in the English legal system will be shown in three stages. First, these rights and freedoms are applicable in domestic law to the extent to which they are implemented by HRA 1998. Second, while these rights and freedoms have vertical direct effect, they have an indirect legal effect on individuals' relations with other private persons. Third, these rights and freedoms are of supreme legal value in the English legal system. Indeed, they have some privileges compared to primary legislation and subordinate legislation. Yet, the judiciary has limited power in protecting these privileges.

3.III.C.2.b.i. Implementation of the Convention rights by the Human Rights Act

The UK is amongst the first countries that signed and ratified the ECHR.[250] Because the UK is a dualist country where signed and ratified international treaties are applicable in domestic law if and to what extent they are implemented, the Convention is not a self-executing source of domestic law.[251] Some 50 years after the signature of the Convention, the Convention rights were transposed into domestic law through Parliamentary Statute. Indeed, HRA 1998, "[a]n act to give further effect to rights and freedoms guaranteed under the European Convention on Human Rights",[252] entered into force in England on 2 October 2000. The only ECHR right that is excluded from the HRA 1998 is the right to an effective remedy in Article 13 of the ECHR.[253] However, this exclusion is by no means that individuals' relevant

[250] The UK Government signed and ratified the Convention on 4 November 1950 and 8 March 1951 respectively. The Convention came into force on 3 September 1953. For further details in relation to the UK's ratification of the Convention, see S Besson, "The reception process in Ireland and the United Kingdom" in H Keller and AS Sweet (eds), *A Europe of Rights: The Impact of the ECHR on National Legal Systems* (OUP 2008) 37-38.

[251] Some authors defended that human rights treaties ought to be self-executing even in dualist systems. Eg. D Beyleveld, "The Concept of Human Right and Incorporation of the European Convention on Human Rights" (1995) P.L. 577. This in fact reflects a broader debate on the dualist idea of separation of domestic law and international law. Some argue that human rights treaties are incompatible with the dualist idea, because human rights treaties are to declare rights of human beings and to apply on their relations, while "dualism … in international legal theory refers to the view that international and municipal law constitute two separate and dichotomous spheres of legal authority with insignificant overlap [and]… international law regulates inter-state conduct". (T Finegan 'Neither Dualism nor Monism: Holism and the Relationship between Municipal and International Human Rights Law' (2011) 2(4) TLT, 477, 478.) In relation to the application of the ECHR in other dualist countries (eg. sector monism in Norway, and moderate dualism in Germany and Italy), see L Wildhaber, 'The European Convention on Human Rights and international law' (2007) 56 International and Comparative Law Quarterly 217.

[252] Introductory text, Human Rights Act 1998.

[253] Section 1(1) of the HRA.

right is not implemented. The HRA determines the ways in which individuals can use their right to an effective remedy.[254] Hence, rights and freedoms enshrined in Section I of the Convention are amongst the sources of domestic law the extent to which they have been incorporated into domestic law by the HRA.

HRA did not incorporate article 32 of the ECHR. However, section 2(1) of the act provides that

> A court or tribunal determining a question which has arisen in connection with a Convention right must take into account any
>
> (a)judgment, decision, declaration or advisory opinion of the European Court of Human Rights,
>
> (b)opinion of the Commission given in a report adopted under Article 31 of the Convention,
>
> (c)decision of the Commission in connection with Article 26 or 27(2) of the Convention, or
>
> (d)decision of the Committee of Ministers taken under Article 46 of the Convention,
>
> whenever made or given, so far as, in the opinion of the court or tribunal, it is relevant to the proceedings in which that question has arisen.

3.III.C.2.b.ii. Vertical direct effect and horizontal indirect effect of the Convention rights and freedoms

The Convention rights and freedoms have vertical direct effect. Section 6(1) of the Act provides that "[i]t is unlawful for a public authority to act in a way which is incompatible with a Convention right". Accordingly, an individual can bring an action against a public authority if the latter's act (or failure to act[255]) constitutes a breach of the former's Convention rights.[256]

A broad definition for 'public authority' is preferred in the Act. Accordingly, courts and tribunals as well as "[a]ny person certain of whose functions are functions of a public nature" are deemed as public authorities.[257] However, there are two exceptions to this broad definition. First, in relation to a particular act, a person is not a public authority just because certain of its' functions are functions of a public nature if the nature of the act is private.[258] Second, "House of Parliament or a person exercising functions in connection with proceedings in Parliament" does not fall under the scope of public authority. Hence, all public authorities apart from the legislative branch of government are required to act in compliance

[254] D Beyleveld and S D Pattinson, 'Horizontal applicability and horizontal effect' (2002) 118 L.Q.R. 623, 631.
[255] Section 6(6) of the HRA.
[256] Section 7(1) of the HRA.
[257] Section 6(3) of the HRA.
[258] Section 6 (5) of the HRA.

with individuals' Convention rights and can be sued before courts when they violate individuals' Convention rights by their action or by their failure to act.

The Convention rights have mediated horizontal effect in English law. An individual A cannot bring an action against another private person B relying on his Convention rights. However, as courts and tribunals are required to act in compliance with individuals' Convention rights, their decisions in cases that relate to individuals' horizontal or vertical relations must not violate individuals' convention rights. Accordingly, courts and tribunals should interpret and give effect to primary legislation and subordinate legislation in a way that is compatible with the Convention rights so far as it is possible to do so.[259] Moreover, the Courts should develop and interpret common law in a way which is compatible with the Convention rights.[260] Hence, while an individual A cannot sue another private person B for breach of his Convention rights, courts and tribunals have some duties to solve disputes between A and B in a way which is compatible with the Convention rights. Similarly, administrative authorities ought to act in compliance with the Convention even when they engage with the regulation of individuals' horizontal relations.

3.III.C.2.b.iii. Supreme legal value of the Convention rights

In dualist theory, domestic law and international law constitute two different legal orders. Therefore, the place of an international treaty in the hierarchy of norms in domestic law depends on the implementing norm. While "[i]t is unlawful for a public authority to act in a way which is incompatible with a Convention right",[261] public authority term in the relevant section of the HRA which implemented the ECHR in domestic law, "does not include either House of Parliament or a person exercising functions in connection with proceedings in Parliament".[262] Hence, the legislative branch of government is excluded from those public authorities given a legal duty to comply with the Convention

[259] Section 3 (1) of the HRA.
[260] Recognition of misuse of private information tort by English Courts to protect individuals' right to privacy (Article 8 ECHR) constitutes an example of interpretation and development of common law by courts in a way which is compatible with the Convention rights. Lord Nicholls, in *Campbell v MGN Ltd* [2004] 2 A.C. 457, para 17, put it that "The time has come to recognise that the values enshrined in articles 8 and 10 are now part of the cause of action for breach of confidence. As Lord Woolf CJ has said, the courts have been able to achieve this result by absorbing the rights protected by articles 8 and 10 into this cause of action: *A v B plc [2003] QB 195 , 202, para 4*. Further, it should now be recognised that for this purpose these values are of general application. The values embodied in articles 8 and 10 are as much applicable in disputes between individuals or between an individual and a non-governmental body such as a newspaper as they are in disputes between individuals and a public authority." Consequently, Lord Nicholls said that "As the law has developed breach of confidence, or misuse of confidential information, now covers two distinct causes of action, protecting two different interests: privacy, and secret ('confidential') information." (*Douglas v Hello! Ltd* (No 3) [2008] AC 1, [255]). Some 6 years later, Court of Appeal held that "misuse of private information should now be recognised as a tort for the purposes of service out the jurisdiction". (*Vidal-Hall and others v Google Inc (Information Commissioner intervening)* [2015] EWCA Civ 311 at [51].)
[261] Section 6(1) of the HRA.
[262] Section 6(3) of the HRA.

rights. Therefore, the Convention rights do not have a direct supra-legislative value. Hence, primary legislation and subordinate legislation may remain valid even when it is incompatible with a Convention right. Moreover, public authorities' duty to act in compliance with the Convention rights does not apply in relation to

> "an act if (a) as the result of one or more provisions of primary legislation, the authority could not have acted differently; or (b) in the case of one or more provisions of, or made under, primary legislation which cannot be read or given effect in a way which is compatible with the Convention rights, the authority was acting so as to give effect to or enforce those provisions".[263]

Hence, acts of public authorities on the basis of primary legislation or subordinate legislation that is not in compliance with the Convention rights may remain legal even when they are incompatible with a Convention right. Yet, HRA established three legal mechanisms to strengthen the Convention rights against primary legislation and subordinate legislation.

First of all, the principle of *lex posterior derogat priori* is limited when it is possible to interpret ulterior primary legislation or subordinate legislation in compliance with the rights and freedoms of individuals in section I of the Convention. Indeed, "[s]o far as it is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with the Convention rights".[264] Hence, the duty of consistent interpretation gives the Convention rights a privileged legal status compared to primary legislation and subordinate legislation.

Second, the courts listed in section 4(5) of the HRA may make a declaration of incompatibility if they are "satisfied (a) that the provision is incompatible with a Convention right, and (b) that (disregarding any possibility of revocation) the primary legislation concerned prevents removal of the incompatibility".[265] While relevant courts can make a declaration of incompatibility, a declaration "does not affect the validity, continuing operation or enforcement of the provision in respect of which it is given; and .. is not binding on the parties to the proceedings in which it is made".[266] Section 10 of the HRA gives some special powers to ministers of crown to make amendments to remove the incompatibility under certain conditions. Hence, there is weak and *a posteriori* conventionality control of primary legislation and subordinate legislation.[267]

[263] Section 6(2) of the HRA.
[264] Section 3 (1) of the HRA.
[265] Section 4(4), HRA 1998.
[266] Section 4(6), HRA 1998.
[267] A Antoine, « Les enjeux de la création d'une cour suprême au Royaume-Uni et la Convention de sauvegarde des droits de l'homme et des libertés fondamentales », (2008) 60(2) Revue internationale de droit comparé 283, 288.

Third, a Minister of the Crown in charge of a Bill in either House of Parliament must make a written statement in relation to the compatibility of the provisions of the Bill with the Convention rights.[268] This provision aims to help legislator be aware of the compatibility or incompatibility of any bill they may legislate. Accordingly, while the legislator is competent to adopt a law that is not compatible with the Convention rights, this should be done by following some further procedural requirements thanks to which the legislator would be aware of this incompatibility beforehand. Section 19(1) of the HRA may be seen as a special version of the Swiss Federal Supreme Court's Jurisprudence Schubert, according to which the federal legislator can enact, with full knowledge of the facts, a domestic rule contrary to international law.[269] The main difference between Section 19(1) of the HRA and the Swiss Federal Supreme Court's Jurisprudence Schubert is that the latter cannot be applied in relation to human rights treaties.[270]

3.III.C.2.c. The intervention of a supranational institution in cases where national law failed to guarantee human beings' ECHR rights

The ECHR differs from traditional international treaties that regulate inter-state conduct in two inter-related senses.[271] First, the Convention regulates the relation between individuals, on the one hand, and private and public persons on the other hand.[272] Second, the ECHR established a supranational mechanism to protect individuals' convention rights that is subsidiary to the protection provided in domestic law. Therefore, the Convention rights constitute supreme legal principles whose protection is further guaranteed at a supranational level in case it was not been protected at the national level.

Member states established legal mechanisms to protect the Convention rights. However, there may still be cases where national law fails to protect one's Convention rights. The Convention provides that, "any person, nongovernmental organisation or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto" has right to bring an action before the ECtHR against a national government that failed to protect his convention rights.[273] Moreover, "[a]ny High Contracting Party may refer to the Court any alleged breach of the provisions of the Convention and the Protocols thereto by another High Contracting Party".[274] The Court's jurisdiction "extend to all matters concerning the interpretation and

[268] Section 19 of the HRA.
[269] ATF 99 Ib 39.
[270] ATF 125 II 417, 424 and ATF 128 IV 201, 205.
[271] Finegan (n,251), 478.
[272] See X and Y v Netherlands (1985) 8 EHRR 235 and M.N. v San Marino (2016) 62 E.H.R.R. 19 at [51] regarding horizontal applicability of article 8 (Right to respect for private and family life). In relation to horizontal applicability of the Convention rights and a long list of cases where horizontal applicability of the Convention rights are recognised by the ECtHR, see B Moutel, « L'Effet Horizontal de la Convention Européenne Des Droits de l'homme en Droit Privé Français: Essai sur la diffusion de la CEDH dans les rapports entre personnes privées » (PhD Thesis, l'Université de Limoges, 25 novembre 2006), Ch 3.
[273] Article 34 of the ECHR.
[274] Article 33 of the ECHR.

application of the Convention" in both individual applications and inter-state cases.[275] Moreover, the ECtHR, a permanent court set up "to ensure the observance of the engagements undertaken by the High Contracting Parties in the Convention and the Protocols thereto",[276] may afford just satisfaction under certain conditions to those whose convention rights are breached. Indeed, "[i]f the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party".[277] "The High Contracting Parties undertake to abide by the final judgment of the Court in any case to which they are parties."[278] Another institution, the Committee of Ministers, supervises the execution of the final judgements of the Court.[279]

3.III.C.3. Conclusion

Banks' making of an SAR interferes with the reported client's ECHR Article 8-1 rights. According to Article 8 of the Convention, laws that aim to the prevention and prosecution of crime can legitimately interfere with one's Article 8-1 ECHR rights under three conditions: the interference is "in accordance with the law", is "necessary in a democratic society" to achieve one or more of the legitimate aims referred to in paragraph 2 of Article 8 of ECHR, one of which is the prevention and prosecution of crime, and there exists sufficient and adequate guarantees against arbitrariness.[280] The ECHR has a privileged status in both English and Swiss laws. Therefore, English and Swiss AML laws relating to the banks' duty and right to make SARs should comply with the listed conditions.

3.IV. Conclusion

This thesis is to investigate AML laws relating to banks' duty and right to make SARs from the perspective of banking clients' right to the protection of personal data. Chapter 2 explored relevant AML laws. This chapter investigated laws that protect banking clients' right to the protection of personal data.

This chapter defended that lawmakers can legitimately require and permit banks to interfere with their clients' privacy rights by making SARs where it is necessary and proportionate to the detection, prevention and prosecution of crime. Chapter 4 investigates the extent to which requiring and permitting banks to report their money laundering suspicions is necessary for the detection, prevention and prosecution of crime. Chapter 5 investigates proportionality of the relevant AML rules. Chapter 5 also

[275] Article 32(1) of the ECHR.
[276] Article 19 of the ECHR.
[277] Article 41 of the ECHR.
[278] Article 46 of the ECHR.
[279] Article 46 of the ECHR.
[280] *M.N. v San Marino* (2016) 62 E.H.R.R. 19 at [73]; Matheron v. France, no. 57752/00, § 35, 29 March 2005.

investigates the way in which AML law's incompliance with data privacy standards affect the effectiveness of relevant AML laws.

CHAPTER 4: THE SUSPICIOUS TRANSACTION REPORTS' PLACE IN THE FIGHT AGAINST CRIME

4.I. Introduction

4.I.A. Arguments

> It is popular to talk about *combating* money laundering and *war* against terrorist financing, but what must be appreciated in such a 'war' is that unlike conventional military conflicts against an opposing military force, a war against money laundering and terrorist financing cannot be fought by government forces alone; the entire intelligence gathering and target acquisition process is in the hands of the private sector. There are no reconnaissance troops scouting forward, no spy planes overhead, it is a war that relies on information supplied by the financial industry and others filing their STRs. [1]

Information privacy laws investigated in chapter 3 suggest that lawmakers can permit banks to interfere with their clients' information privacy rights by making STRs if the interference is prescribed by law, and such interference respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard the prevention, investigation, detection or prosecution of criminal offences. This chapter defends that law enforcement agencies cannot successfully fight against money laundering and underlying offences without information supplied by the banking industry filing their STRs.[2]

Countries willing to fight against economic crime adopted confiscation measures to deprive the offenders of the proceeds of their crime. Moreover, they criminalised money laundering to punish those who conceal or disguise the identity of illegally obtained proceeds.[3] As a reaction to these legal institutions, economic criminals started to develop sophisticated and hard-to-detect money laundering schemes by misusing banking products and services. Law enforcement agencies willing to confiscate criminal money and punish money launderers adopted a follow-the-money approach, which suggests that law enforcement agencies should follow suspicious money in order to detect economic crime, criminal money and economic criminals. Law enforcement agencies willing to detect criminal money

[1] P A Gallo and C C Juckes, 'Threshold transaction disclosures: access on demand through latent disclosure rather than reporting' (2005) 8(4) J.M.L.C. 328, 328.
[2] Ibid.
[3] "Money Laundering", Interpol web site, <https://www.interpol.int/Crime-areas/Financial-crime/Money-laundering> accessed 14 June 2018.

and economic crime should attach great importance to the STRs produced by banks due to two reasons. First, banking staff have the capacity to distinguish their client's regular, unusual and suspicious financial transactions and activities. Second, law enforcement agencies should diligently follow suspicious banking transactions because economic criminals often misuse banking services and products in laundering proceeds of crime.

4.I.B. Key concepts : Economic crime and economic criminal

There are several terms employed in the criminal law literature such as 'economically motivated crime', 'acquisitive crime' and 'financial market crime' in addition to 'financial crime' and 'economic crime'. Although the economic crime term has been growing in use,[4] there is no clear agreement on its' definition.[5] Researchers, governmental authorities and international organisations regroup various crimes within the overall rubric of economic crime.[6] According to Gilligan, the position of individuals and agencies when they need to define economic or financial crime is similar to a famous quote from Justice Potter Stewart of the US Supreme Court, who said of obscene material that perhaps he could not intelligibly define what it is, but he knows it when he sees it.[7]

Economic crime in this thesis refers to any crime by which an offender, real or legal person, obtained acquisitive gain or advantage regardless of whether his primary aim was to obtain such profit or advantage or not. Thus, 'economic crime' is broader than 'economically motivated crime'.[8] Consequently, the economic criminal term refers to any offender, real or legal person, who obtained acquisitive gain or advantage from its' criminal activity regardless of whether its primary aim was to receive such profit or advantage or not. This thesis preferred a broad definition because any offender who gained proceeds from their illicit activity may involve in money laundering, and this thesis investigates AML laws.[9]

[4] M Levi, 'Foreword: some reflections on the evolution of economic and financial crime' in B Rider (ed), *Research Handbook on International Financial Crime* (Edward Elgar Publishing 2015), xxiii.
[5] W Trupman, 'The characteristics of economic crime and criminals' in B Rider (ed), *Research Handbook on International Financial Crime* (Edward Elgar Publishing 2015), 5.
[6] G G Gilligan, 'Financial crime: a historical perspective' in B Rider (ed), *Research Handbook on International Financial Crime* (Edward Elgar Publishing 2015), 34; and see some examples in Trupman (n.5), 5.
[7] Gilligan (n,6), 33 with reference to *Jacobellis v Ohio*, 84 S. Ct. 1676 [1964].
[8] Trupman (n.5), 4.
[9] For a similar definition of the economic crime term elaborated on the basis of a similar criterion, see U Cassani, « Le blanchiment d'argent, un crime sans victim? » in N Schmid et al. (eds), *Wirtschaft und Strafrecht: Festschrift* (Schulthess 2001), 395.

4.II. Confiscation measures

4.II.A. Introduction

The General Assembly of the United Nations proclaimed the Universal Declaration of Human Rights 1948 (UDHR 1948) as 'a common standard of achievement for all peoples and all nations', with the strong support of the international community.[10] The UDHR 1948 recognised everyone's right "to a social and international order in which the rights and freedoms set forth in … [the] Declaration can be fully realized".[11] Therefore, countries ready to affect the UDHR 1948 should make an effort for establishing a society where everyone's rights and freedoms are respected.[12]

Proceeds of crime term may be defined as the economic gain or advantage an offender obtained by attacking and seriously harming another person's or other persons' rights and freedoms.[13] Legal systems willing to give effect to the rights and freedoms enshrined in the UDHR 1948 are justified in adopting confiscation measures because depriving offenders of the proceeds of crime is internally and externally instrumental toward establishing a society where everyone's rights and freedoms are respected.[14] The United Nations' Vienna Convention 1988 and the Palermo Convention 2000 require countries to adopt confiscation measures. These conventions have 191 and 190 state parties, respectively.[15]

Depriving offenders of the proceeds of crime is internally instrumental toward establishing a society where everyone's rights and freedoms are respected. Law enforcement agencies can restore the occurrent pre-crime equality of rights by depriving the offender of the proceeds of crime. The victim of a criminal offence may be a specified person or a community of people. Where the victim is a specified person, the proceeds of crime should primarily be used to recover the damage of that specified person. For instance, if A stole 10 pounds from B, the occurrent pre-crime equality of goods may be restored by giving the extra 10 pounds possessed by offender B to victim A. Where the victim is the community

[10] As its preamble stressed out, the Universal Declaration was proclaimed by the General Assembly "as a common standard of achievement for all peoples and all nations". The UDHR 1948 was ratified through a proclamation by the General Assembly of the United Nations in 1948 with a count of 48 votes to none with only 8 abstentions. In relation to the legal value of the UDHR, see M V Alstine, 'The Universal Declaration and Developments in the Enforcement of International Human Rights in Domestic Law', (2009) 24 Md. J. Int'lL 63, 64. and J von Bernstorff, 'The Changing Fortunes of the Universal Declaration of Human Rights: Genesis and Symbolic Dimensions of the Turn to Rights in International Law' (2008) 19(5) EJIL 903, 904.

[11] Article 28 of the UDHR.

[12] See D Beyleveld and R Brownsword, *Law as a Moral Judgment* (Sheffield Academic Press 1994), ch 5; D Beyleveld, 'The Principle of Generic Consistency as the Supreme Principle of Human Rights' (2012) 13 Human Rts. Rev. 1, 6; and A Gewirth, *Reason and Morality* (University of Chicago Press 1978), 272-327.

[13] In relation to the definition of criminal offence, see T Brooks, *Punishment* (Routledge 2012), 16; S P Brown, 'The moral justification of retributive punishment by reference to the notion of balance' (PhD thesis, University of Sheffield 1998), 29.

[14] In relation to internal and external instrumental justification of legal rules, see Gewirth (n.12), 290-312.

[15] See UN treaties website, <https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=VI-19&chapter=6&clang=_en> and <https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html> accessed 30 September 2021.

of people rather than a particular person, as is the case in the offences of terrorist financing, drug trafficking and tax evasion, the occurrent pre-crime equality of rights may be restored by using criminal proceeds to recover the damages of the society.

Depriving offenders of the proceeds of crime is externally instrumental toward establishing a society where everyone's rights are respected.[16] First of all, confiscation terms can deter people from committing an economically motivated crime. Lord Woolf CJ, in *R v Benjafield* put it that "[i]f offenders are likely to lose their ill-gotten benefits, then this in itself will be a significant deterrent to the commission of further offences."[17] In another case, his lordship submitted that[18]

> one of the most successful weapons which can be used to discourage offences that are committed in order to enrich the offenders is to ensure that if the offenders are brought to justice, any profit which they have made from their offending is confiscated.

Second, confiscation terms give law enforcement agencies a chance to dismantle offenders of the capacities, abilities and sources to commit further offences. Criminal organisations, particularly terrorist groups, cannot survive without money.[19] Therefore, confiscation terms play an essential role in the fight against organised crime. In particular, confiscation terms may serve to "starve the terrorists of funding, turn them against each other [. . .] and bring them to justice".[20]

Countries willing to fight against economic crime should adopt confiscation terms depriving offenders of the proceeds of crime. The FATF, in its' recommendation 4, advised countries to adopt confiscation measures. English and Swiss lawmakers affected the FATF's relevant recommendation.

4.II.B. The FATF recommendations

The FATF recommends countries to adopt confiscation measures. According to the FATF's recommendation 4 on 'confiscation and provisional measures', countries should

> adopt measures … to enable their competent authorities to freeze or seize and confiscate … (a) property laundered, (b) proceeds from, or instrumentalities used in or intended for use in money laundering or predicate offences, (c) property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations, or (d) property of corresponding value.[21]

---

[16] G S Becker, 'Crime and Punishment: An Economic Approach' (1968) J. Pol. Econ. 76, 91.
[17] *R v Benjafield* [2001] 3 WLR 74, at [43].
[18] *R v Sekhon* [2002] EWCA Crim 2954, at [1].
[19] V Chadha, *Lifeblood of Terrorism: Countering Terrorism Finance* (Bloomsbury Publishing India 2015), 17.
[20] Executive Order 13224 of 2001 (2001), <http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/print/20010924-1.html> 1 October 2018.
[21] Recommendation 4. FATF (2012-2020), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, 19, <www.fatf-gafi.org/recommendations.html> 10 June 2021.

Moreover, countries are recommended to

> consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction (non-conviction based confiscation), or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.[22]

The FATF defines non-conviction based confiscation as "confiscation through judicial procedures related to a criminal offence for which a criminal conviction is not required".[23] The FATF's recommendation 4 highlights that confiscation measures must not prejudice *bona fide* third parties' rights.[24]

The FATF also recommends countries to adopt provisional measures to guarantee the effectiveness of the confiscation measures.[25] Provisional measures

> should include the authority to: … carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; [and] take steps that will prevent or void actions that prejudice the country's ability to freeze or seize or recover property that is subject to confiscation.[26]

4.II.C. English Law

Part 2 of POCA 2002 specified criminal confiscation measures to dismantle and disrupt the offenders by taking the profit out of crime.[27] Moreover, there are civil recovery terms in Part 5 of the act to seal the gaps of criminal confiscation. The Cabinet Office report explained the reasons for confiscation powers as follows:[28]

> Leaving illegal assets in the hands of criminals damages society. First, these assets can be used to fund further criminal activity, leading to a cycle of crime that plagues communities. Second, arrest and conviction are not enough to clamp down on crime; they leave criminals free to return to their illegal enterprises, or even to continue their 'business' from prison.

---

[22] Ibid.
[23] "General Glossary", FATF (n.21), 122.
[24] Recommendation 4, FATF (n.21), 12.
[25] Ibid.
[26] Ibid.
[27] Part 2 of POCA 2002 specifies criminal confiscation terms to be applied in England and Wales, while parts 3 and 4 specify criminal confiscation terms to be applied in Scotland and Northern Ireland, respectively. For a comparison of these parts, see J Fisher QC, 'UK Part IV: Confiscating the proceeds of crime' in M Simpson, N Smith and A Srivastava (eds) *International guide to money laundering law and practice* (3rd edition, Bloomsbury Professional 2010), 170.
[28] *Recovering the Proceeds of Crime* (Performance Innovation Unit, Cabinet Office, June 2000.

> And third, it simply is not right in modern Britain that millions of law-abiding people work hard to earn a living, whilst a few live handsomely off the proceeds of crime.

English law is 'compliant' with the requirements of the FATF's recommendation 4.[29]

4.II.C.1. Criminal Confiscation

Part 2 of POCA 2002 lists strong post-conviction confiscation measures, which are even strengthened with some assumptions to be made where the offender has a criminal lifestyle. A defendant is presumed to have a criminal lifestyle if the offence for which he has been convicted is, among others, a money laundering offence specified in sections 327 [concealing etc.] or 328 [arrangement] of POCA 2002.[30]

Criminal confiscation is principally conviction-based. The Crown Court[31] must proceed a confiscation order where the following two conditions are met: (i) the defendant is convicted of an offence or offences in proceedings before the Crown Court; or he is committed to the Crown Court for sentence in respect of some listed offences,[32] and (ii) the prosecutor asks the court to proceed under section 6 of POCA 2002, or the court believes it is appropriate for it to do so.[33] There are exceptions recognised in sections 27 and 28 of POCA 2002 to prevent the absconding offenders from keeping criminal money. While section 27 applies to the absconding defendants convicted or committed, section 28 applies to the absconding defendants neither convicted nor acquitted.

A confiscation order "impose[s] on a defendant the obligation to pay a sum of money that reflects the benefit he received from his criminal conduct."[34] According to section 76(1), "[c]riminal conduct is conduct which (a) constitutes an offence in England and Wales, or (b) would constitute such an offence if it occurred in England and Wales." A person benefits from his criminal conduct if he obtains property[35] or pecuniary advantage[36] as a result of or in connection with the conduct. The offender is to be taken to obtain pecuniary advantage as a result of or in connection with the conduct a sum of money equal to the value of the pecuniary advantage.[37]

---

[29] FATF (2018), Anti-money laundering and counter-terrorist financing measures – United Kingdom, Fourth Round Mutual Evaluation Report, FATF, Paris, France, 179, <http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-kingdom2018.html> 10 June 2021.
[30] Section 75, POCA 2002 and section 2 of Schedule 2 of POCA 2002.
[31] In relation to the Secretary of State's authority to make an order enabling magistrates' courts in England and Wales to make confiscation orders under Part 2 of the Proceeds of Crime Act 2002 in a sum less than 10,000 GBP, see section 97 of SOCPA.
[32] Listed offences are offences under section 3, 3A, 3B, 3C, 4, 4A or 6 of the Sentencing Act and under section 70 of POCA 2002. See section 6(2) of POCA 2002.
[33] Section 6(3), POCA 2002.
[34] Fisher (n.27), 155.
[35] Section 76(4), POCA 2002.
[36] Section 76(5), POCA 2002.
[37] Section 76(5), POCA 2002.

Where the court decides that the defendant has benefited from his criminal conduct, it must determine the recoverable amount and make a confiscation order requiring the defendant to pay that amount. The court must decide the following questions on a balance of probabilities: whether the defendant has benefited from his criminal conduct and what is the recoverable amount.[38] The recoverable amount

> is an amount equal to the defendant's benefit from the conduct concerned. But if the defendant shows that the available amount is less than that benefit the recoverable amount is (a) the available amount, or (b) a nominal amount, if the available amount is nil".[39]

Section 9 explains the recoverable amount and protects the rights of *bona fide* third parties as follows:[40]

> (1)For the purposes of deciding the recoverable amount, the available amount is the aggregate of—
>
> (a)the total of the values (at the time the confiscation order is made) of all the free property then held by the defendant minus the total amount payable in pursuance of obligations which then have priority, and
>
> (b)the total of the values (at that time) of all tainted gifts.
>
> (2)An obligation has priority if it is an obligation of the defendant—
>
> (a)to pay an amount due in respect of a fine or other order of a court which was imposed or made on conviction of an offence and at any time before the time the confiscation order is made, or
>
> (b)to pay a sum which would be included among the preferential debts if the defendant's bankruptcy had commenced on the date of the confiscation order or his winding up had been ordered on that date.

A confiscation order against a defendant who has a criminal lifestyle imposes on the defendant the obligation to pay a sum of money that reflects the benefit he received from his general criminal conduct.[41] According to section 76(2), "general criminal conduct of the defendant is all his criminal conduct".

If the court decides that the defendant does not have a criminal lifestyle, the confiscation order imposes on the defendant an obligation to pay a sum of money that reflects the benefit he received from his particular criminal conduct. Section 76(3) explaines particular criminal conduct as follows:

> Particular criminal conduct of the defendant is all his criminal conduct which falls within the following paragraphs—
>
> (a)conduct which constitutes the offence or offences concerned;

[38] Subsection 7 of section 6 of POCA 2002. See also R v Granger [2007] EWCA Crim 139 at [13] and R v Barnham [2005] EWCA Crim 1049 at [40]-[41].
[39] Sections 7 (1) and (2), POCA 2002.
[40] FATF (n.29), 179. In relation to tainted gifts, see M Sutherland Williams, M Hopmeier and R Jones, *Millington and Sutherland Williams on the Proceeds of Crime* (4th ed, OUP 2013), [9.141]- [9.147].
[41] Fisher (n.27), 155.

(b)conduct which constitutes offences of which he was convicted in the same proceedings as those in which he was convicted of the offence or offences concerned;
(c)conduct which constitutes offences which the court will be taking into consideration in deciding his sentence for the offence or offences concerned.

There are three scenarios in which a defendant is presumed to have a criminal lifestyle.[42] First, a defendant is presumed to have a criminal lifestyle if the offence for which he has been convicted is an offence specified in Schedule 2 of the POCA 2002, which includes, among others, money laundering offences specified in sections 327 [concealing etc.] and 328 [arrangement] of POCA 2002.[43] Second, a defendant is presumed to have a criminal lifestyle if the offence for which he has been convicted constitutes conduct forming part of a course of criminal activity.[44] Third, a defendant is presumed to have a criminal lifestyle if the offence for which he has been convicted was committed over a period of at least six months and the defendant has benefited from the conduct which constitutes the offence. However, a crime does not satisfy the test in the last two scenarios if the defendant obtains a relevant benefit of less than £5000.[45] The court must decide whether the defendant has a criminal lifestyle on a balance of probabilities.[46]

A defendant who has a criminal lifestyle is assumed to have gained his life from the criminal activity for a period of time starting with "the first day of the period of six years ending with the day when proceedings for the offence concerned were started against the defendant".[47] The Court shall make four 'draconian assumptions' where the defendant has a criminal lifestyle.[48] First, any property transferred to the defendant at any time after the relevant day (ie. "the first day of the period of six years ending with the day when proceedings for the offence concerned were started against the defendant"[49]) is assumed to have been "obtained by him as a result of his general criminal conduct, and at the earliest time he appears to have held it".[50] Second, it is assumed that "any property held by the defendant at any time after the date of conviction was obtained by him as a result of his general criminal conduct, and at the earliest time he appears to have held it."[51] Third assumption is that "any expenditure incurred by the defendant at any time after the relevant day was met from property obtained by him as a result of his general criminal conduct."[52] Fourth, it is assumed that "for the purpose of valuing any property obtained

[42] Sections 75(1)-(2), POCA 2002.
[43] Section 2 of Schedule 2 of POCA 2002.
[44] See section 75(3) of POCA 2002.
[45] Section 75(4), POCA 2002.
[46] Subsection 7 of section 6 of POCA 2002. See also R v Granger [2007] EWCA Crim 139 at [13] and R v Barnham [2005] EWCA Crim 1049 at [40]-[41].
[47] Section 10(8), POCA 2002.
[48] Fisher (n.27), 158.
[49] Section 10(8), POCA 2002.
[50] Section 10(2), POCA 2002.
[51] Section 10(3), POCA 2002.
[52] Section 10(4), POCA 2002.

(or assumed to have been obtained) by the defendant, he obtained it free of any other interests in it".[53] These presumptions may have severe effects on the parties to which they apply.[54] However, it is worth mentioning that "the court must not make a required assumption in relation to particular property or expenditure if the assumption is shown to be incorrect, or there would be a serious risk of injustice if the assumption were made".[55]

4.II.C.2. Civil recovery

Criminal confiscation may be processed following a criminal proceeding. Yet, it is not always possible to commence criminal proceedings. For instance, the offender may have kept himself distant from the crime he was controlling, or he may be outside the UK. Similarly, the offender may die, leaving recoverable assets. Where the Crown Prosecution Service decides not to commence criminal proceedings, civil recovery terms may be used.[56]

Part 5 of POCA 2002 deals with the recovery by a civil action of property obtained through unlawful conduct, whether or not any proceedings have been brought for an offence in connection with the property.[57] Hence, civil recovery orders seal the gaps in criminal confiscation.

"Proceedings for a recovery order may be taken by the enforcement authority in the High Court against any person who the authority thinks holds recoverable property".[58] The claimant enforcement authority must prove on a balance of probabilities that any matters alleged to constitute unlawful conduct have occurred.[59]

Recoverable property is 'property obtained through unlawful conduct'.[60] Conduct occurring in any part of the UK is unlawful conduct if it is unlawful under that part's criminal law.[61] Conduct which (a) occurs in a country or territory outside the UK and is unlawful under the criminal law applying in that country or territory, and (b) if it occurred in a part of the United Kingdom, would be unlawful under the criminal law of that part, is also unlawful conduct.[62] Property is obtained through unlawful conduct if one obtained it by or in return for the unlawful conduct (whether his own conduct or another's). Tracing

[53] Section 10(5), POCA 2002.
[54] Fisher (n.27), 158.
[55] Section 10(6), POCA 2002.
[56] Fisher (n.27), 171.
[57] Section 240(2), POCA2002.
[58] Section 243 (1), POCA2002.
[59] Section 241(3), POCA 2002.
[60] Section 304(1), POCA 2002.
[61] Section 241(1), POCA 2002.
[62] Section 241(2), POCA 2002. In relation to the exceptions of the double criminality test, see sections 241(2A) and 241A of POCA 2002.

property, which represents the original property obtained through unlawful conduct, and mixed property may also be recoverable property.[63]

Section 308(1) protects the rights of *bona fide* third parties as follow:[64]

> If—
>
> (a)a person disposes of recoverable property, and
>
> (b)the person who obtains it on the disposal does so in good faith, for value and without notice that it was recoverable property,
>
> the property may not be followed into that person's hands and, accordingly, it ceases to be recoverable.

4.II.C.3. Provisional measures

The Crown Court can make restraint orders to protect the

> value for the time being of realisable property being made available (by the property's realisation) for satisfying any confiscation order that has been or may be made against the defendant, and in a case where a confiscation order has not been made, with a view to securing that there is no diminution in the value of realisable property.[65]

A restraint order may be made where a criminal investigation has been started or proceedings for an offence have been started and not concluded. To make a restraint order, the court must have reasonable cause to believe that the alleged offender has benefited from his conduct.[66] A restraint order prohibits a specified person from dealing with any realisable property held by him.

4.II.D. Swiss law

Swiss Criminal Code 1937 (SCC 1937) specified forfeiture terms to dismantle and disrupt the offenders by taking the profit out of crime. Swiss law is rated 'largely compliant' with the requirements of the FATF's recommendation 4.[67]

---

[63] In relation to tracing property and mixed property, see sections 305 and 306 of POCA 2002, respectively.
[64] See sections 266, 281 and 308 of POCA 2002.
[65] Section 69(2), POCA 2002.
[66] Fisher (n.27), 148.
[67] FATF (2016), Anti-money laundering and counter-terrorist financing measures - Switzerland, Fourth Round Mutual Evaluation Report, FATF, Paris, France, 162 <www.fatf-gafi.org/publications/mutualevaluations/documents/mer-switzerland-2016.html> 10 June 2021; and FATF (2020), Anti-money laundering and counter-terrorist financing measures - Switzerland, Enhanced Follow-up Report & 2nd Technical Compliance Re-Rating, FATF, Paris, 11 <http://www.fatf-gafi.org/publications/mutualevaluations/documents/fur-switzerland-2020.html>.

4.II.D.1. Forfeiture terms

Forfeiture terms specified in SCC 1937 involve objective measures, not penalties.[68] Therefore, forfeiture claims may be applied regardless of the criminal liability or conviction of a particular person.[69] Indeed, any asset obtained directly or indirectly by means of criminal activity may be subject to forfeiture terms,[70] as far as the prosecuting authority can prove all objective and subjective elements of the underlying offence,[71] as well as the paper trail of the criminal property[72].

The court shall order the forfeiture of assets (i) that have been acquired through the commission of an offence,[73] (ii) that are intended to be used in the commission of an offence or as payment therefor,[74] or (iii) that are subject to the power of disposal of a criminal organisation.[75] Offence covers both felonies (ie. offences that carry a custodial sentence of more than three years[76]), and misdemeanours (ie. offences that carry a custodial sentence not exceeding three years or a monetary penalty[77]). Swiss courts are authorised to order the forfeiture of criminal assets where they are allowed to prosecute the crime by which the criminal property at stake was obtained.[78]

The scope of the recoverable benefit is a controversial subject in Swiss legal literature. The Federal Supreme Court applies gross calculations for generally prohibited activities such as drug trafficking, money laundering, and terrorist financing. For acts that are permitted in principle but are not permitted

[68] Cour de cassation, Geneve, 22 novembre 1996, *SJ* 1997 186 ss; M. Hirsig-Vouilloz « Le nouveau droit suisse de la confiscation pénale et de la créance compensatrice (art. 69 a 73 CP) » AJP 2007, 1376, Art 70 N9; C Lombardini, *Banques et blanchiment d'argent* (3rd éd, Schulthess 2016), 130.
[69] In relation to application of confiscation measures in cases where no one is committed, see ATF 128 IV 145 ss, 151/*JdT* 2004 IV 32, *SJ* 2002 I 656; TF, 8 juillet 2014, 6B_864/2013; TF, 7 fevrier 2005, 6P.142/2004; TF, 25 fevrier 2015, 6B_508/2014. See S Giroud and H Rordorf-Braun, *Droit suisse des sanctions et de la confiscation international* (Helbing Lichtenhahn Verlag 2020), 23.
[70] Lombardini (n.68), 130.
[71] TF, 8 fevrier 2006, 6P.117/2005, cons. 2.3 and TF, 8 fevrier 2006, 6S.265/2005, cons 4.3.2; Cour de cassation, Geneve, 22 novembre 1996, *SJ* 1997 186 ss; Lombardini (n.68), 130; O Abo Youssef and L Ruckstuhl "Switzerland" in *The international comparative legal guide to Anti-money laundering 2018* (Global Legal Group, 2018) < https://iclg.com/practice-areas/anti-money-laundering-laws-and-regulations/switzerland> 20 January 2019.
[72] TF, 26 mai 2003, 6S.709/2000 and 6S.710/2000, cons. 6.3; TF, 14 novembre 2007, 6B_369/2007; TF, 24 mars 2013, 1B_711/2012.
[73] Article 70, SCC 1937.
[74] Article 70, SCC 1937.
[75] Article 72, SCC 1937.
[76] Article 10(2), SCC 1937.
[77] Article 10(3), SCC 1937.
[78] See articles 3 to 7 and 305bis(3) of SCC 1937 and article 24 of Federal Act on Narcotics and Psychotropic Substances. In relation to the application of articles 3 to 7 SCC in conjunction with article 70 of SCC, see ATF 128 IV 145/*JdT* 2004 IV 32, *SJ* 2002 I 565; ATF 134 IV 185, *SJ* 2008 I 325. In relation to the application of article 305bis(3) of SCC in conjunction with article 70 of SCC, see TPF, 16 mars 2015, BB.2014.157, cons, 3.1. For further details, see G Pavlidis, *Confiscation internationale: instruments internationaux, droit de l'Union Européenne, droit Suisse* (Schulthess 2012), 196.

in specific instances as being related to an offence, such as a contract that has been obtained through corrupt means, the court applies net calculations, where the production costs are deducted.[79]

"If the amount of the assets to be forfeited cannot be ascertained, or may be ascertained only by incurring a disproportionate level of trouble and expense, the court may make an estimate".[80] A forfeiture order is unnecessary if the assets were passed on to the person harmed to restore the prior lawful position.[81]

If the assets subject to forfeiture are no longer available, the court may uphold a claim for compensation by the State in respect of a sum of equivalent value. This claim may be enforced against a third party only if he is not a *bona fides* third party.[82] Bona fides third party is defined as one who "has acquired the assets in ignorance of the grounds for forfeiture, provided he has paid a consideration of equal value therefor or forfeiture would cause him to endure disproportionate hardship".[83] It is worth mentioning that these two conditions (ie. 1. he has acquired the assets in ignorance of the grounds for forfeiture and 2. he has paid a consideration of equal value therefor or forfeiture would cause him to endure disproportionate hardship) are cumulative,[84] and the burden of proving that at least one of the conditions is not met rests with the prosecuting authority.[85]

4.II.D.2. Provisional measures

According to article 263 of Swiss Criminal Procedure Code of 2007 (SCPC 2007), items and assets belonging to an accused or to a third party may be seized if it is expected that the items or assets will be used as (i) security for procedural costs, monetary penalties, fines or damages; (ii) will have to be returned to the persons suffering harm; (iii) will have to be forfeited. According to article 263 of SCPC 2007,

> Seizure shall be ordered on the basis of a written warrant containing a brief statement of the grounds. In urgent cases, seizure may be ordered orally, but the order must thereafter be confirmed in writing. Where there is a risk in any delay, the police or members of the

[79] ATF 124 I 6, RDAF 1999 I 508; ATF 123 IV 70/*JdT* 1998 IV 159; TF, 22 septembre 2006, 6S.302/2006; TF, 28 decembre 2006, 6S.426/2006; TF, 28 avril 2003, 1P.120/2003; *SJ* 2007 I 271. For a decision where the Federal Supreme Court applied net calculation for a generally prohibited activity, see TF, 23 juin 2015, 6B_988/2014, 6B_989/2014, 6B_990/2014. See also Hirsig-Vouilloz (n.68), 1376; B Bertossa, « Confiscation et corruption, Quelques réflexions sur la confiscation des avantages obtenus par le corrupteur actif », SJ 2009 II, 379; Abo Youssef and Ruckstuhl (n.71); Lombardini (n.68), 122; Pavlidis (n.79), 213.
[80] Article 70, SCC 1937.
[81] Article 70, SCC 1937 ; TF, 11 mai 2009, 6B_1035/2008.
[82] Article 71, SCC 1937.
[83] Article 70(2), SCC 1937. In relation to the definition of bona fides third party, see also TF, 19 septembre 2007, 1S.32/2006.
[84] S Nadelhofer Do Canto, « Quelques aspects de la confiscation selon l'art 70 al. 2 CP» RPS, 2008, 312.
[85] Hirsig-Vouilloz (n.68), N 38.

public may provisionally seize items or assets on behalf of the public prosecutor or the courts.

4.III. The offence of money laundering

4.III.A. Introduction

As explained above, law enforcement agencies disrupt economic criminals by confiscating criminal money. Criminals, therefore, make every endeavour to benefit from the criminal proceeds safely. One method to benefit from proceeds of crime without disruption may be concealing or cleansing its source origin. Legal systems criminalised concealing or disguising the identity or the source origin of the criminal proceeds.[86] It is worth mentioning that money laundering is a relatively recently criminalised offence and has been defined differently in diverse legal systems.

4.III.B. A short history of the offence of money laundering

One who obtains property by committing a crime needs to take measures to benefit without disruption from the proceeds of the crime. An ancient method of using criminal proceeds without disruption is concealing or cleansing its source origin.[87] This may be achieved in many different ways, depending on the nature of the proceeds and existing policing methods. An axe thief might conceal the illicit source origin of the stolen axe by doing some changes on the form of the stolen axe to the extent its' previous owner can no more identify it. A drug lord seems to need sophisticated international money laundering structures to hide the source origin of illicit money.[88]

While economic criminals have long needed to take measures to benefit without disruption from the proceeds of their criminal activity, nobody looked at these measures as a crime as such prior to the 20th century.[89] Even the term 'money laundering' was born in the 20th century.[90] By criminalising money laundering, legal systems aim to fight successfully against economic crime.

---

[86] "Money Laundering" (n3).
[87] W H Muller, 'Anti-Money Laundering – A short story' in W H Muller, C H Kalin and J G Goldworth (eds), *Anti-money laundering – International law and practice* (John Wiley & Sons 2007), 3.
[88] Eg. Colombian drug lord Jose Santacruz-Londono had been cleansing his illegal money in the late 1980's and early 1990's with a famously complex money laundering scheme created by a Harvard-educated economist Franklin Jurado. "Special Future- Money Laundering" (UN Special Futures, UN General Assembly Special Session on the World Drug Problem 8-10 June 1998) <https://www.un.org/ga/20special/featur/launder.htm> 18 December 2018.
[89] Muller (n.87), 3.
[90] J Kranacher, R Riley and J T Wells, *Forensic Accounting and Fraud Examination* (Wiley 2011), 112.

Anti-drug trafficking laws of the 1970s and 1980s are the direct ancestors of modern anti-money laundering laws.[91] Starting from the 1970s, law enforcement authorities have been given additional powers that helped them fight against drug smuggling.[92] First, courts were given the power to seize drug and money gained from drug trafficking.[93] Second, 'laundering' money obtained from drug trafficking was recognized as a separate criminal offence.[94] For instance, English law criminalized assisting another to retain the benefit of drug trafficking, knowing or suspecting that the other person carries on or has carried on drug trafficking or has benefited from drug trafficking.[95]

Lawmakers consequently widened the scope of the prohibited acts. Article 3.1 of the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances adopted in 1988 (the Vienna Convention) provided that laundering drug property crimes should include (i) converting or transferring property knowing that such property is derived from drug trafficking, (ii) concealing or disguising the true nature, source, location, disposition, movement, rights with respect to or property of

---

Money laundering term has arguably been originated with a famous American gangster, Al Capone, who allegedly had been cleansing his illegally obtained money via Laundromats. His tainted money was arguably integrated into the legal economy as if it was obtained through legitimate business sales from the laundromats. American police was not successful in proving a long list of crimes were committed or abetted by Al Capone. Yet, he was indicted with tax evasion and convicted to imprisonment for 11 years. (Capone v. United States, 51 F.2d 609 (7th Cir. 1931). Because Al Capone was not indicted for a money laundering offence, it is not possible to accept this case as the starting point for the offence of money laundering. However, by showing the importance of a follow the money approach for an effective fight against organized crime syndicates, this case had a significant effect on the evolution of economic criminal law. Muller (n.87), 3.

Some European authors, on the other hand, find the basis of money laundering term "in the 1970s in the context of ransom monies… [which] the [law enforcement] authorities routinely recorded the serial numbers of bank notes that were paid out to obtain the release of the victims of [hostage taking and kidnapping] crimes". (N Capus, 'Country Report: Combating money laundering in Switzerland' in M Pieth and G Aiolfi (eds), *A Comparative Guide to Anti-Money Laundering* (Edward Elgar 2004), 128). Knowing that the authorities were tracing the registered bank notes, "the perpetrators … sought to 'wash' the proceeds of their crimes so that the money could be returned to circulation" (Capus (n90), 128). While tracing the registered bank notes was a method used by law enforcement to find offenders, laundering criminal money had not been accepted as a separate criminal offence. Hence, in 1970's Europe, money laundering was no more than a method employed by offenders who were chased by law enforcement authorities that follows the money.

The earliest judicial acknowledgment of money laundering term is a 1982 American case (US v $4,255,625.39 (1982) 551 F sup.314, see N Ryder 'Introduction' in N Ryder (ed.) *White collar crime and risk – Financial crime, corruption and the financial crisis* (Palgrave Macmillan 2018), 2). In fact, there were prior Swiss and British laws that recognized dealing with proceeds of some crimes as a separate offence. Yet, these laws did not use money laundering term. Section 22 (1) of the Theft Act 1968 (UK) predicted penalties for those who received or dealt with stolen property ('receiving or dealing with stolen goods' offence), while laundering proceeds of crime was a punishable offence in Switzerland "if the proceed arose from a crime against property (such as theft, robbery, fraud etc.)" (Capus (n90), 128). These laws may be accepted as the late ancestors of AML laws.

[91] Examples: the UK, USA, France, Canada and Switzerland. D P Murphy, 'International developments surrounding the proceeds of crime (money laundering) and terrorist financing act' in *Dirty Money: civil and criminal aspects of money-laundering* - Conference Meredith Lectures 2002, Edition Tvon Blais, 2003, 1-7; G Stessens, *Money Laundering – A new international law enforcement model* (Cambridge University Press 2000), 3-6, 82-85; M Pieth, 'International standards against money laundering' in M Pieth and G Aiolfi (eds), *A Comparative Guide to Anti-Money Laundering* (Edward Elgar 2004), 3-12; and Lombardini (n.68), 1-3.

[92] J Ulph, *Commercial Fraud : Civil Liability, Human Rights and Money Laundering* (OUP 2006), 125.

[93] See the UK Misuse of Drugs Act 1971 and Drug Trafficking Offences Act 1986 in relation to English courts' power to seize drug and proceeds obtained from drug trafficking respectively.

[94] B Unger, 'Money Laundering Regulation: from Al Capone to Al Qaeda' in B Unger and D vaan der Linde (eds), *Research Handbook on Money Laundering* (Edward Elgar 2013), 23.

[95] Section 24 of Drug Trafficking Offences Act 1986.

such property, (iii) as well as acquiring, possessing or using such property. The forty recommendations of the Financial Action Task Force on money laundering released in 1990 advised countries to "criminalize drug money laundering as set forth in the Vienna Convention".[96] The UK transposed the Vienna Convention into domestic law with section 14 of the Criminal Justice (International Cooperation) Act 1990.[97]

Starting from the 1990s, international organizations advised countries to extend laundering offences to other economic crimes. The forty recommendations of the Financial Action Task Force on money laundering 1990 advised countries to[98]

> consider extending the offense of drug money laundering to any other crimes for which there is a link to narcotics; an alternative approach is to criminalize money laundering based on all serious offenses, and/or on all offenses that generate a significant amount of proceeds, or on certain serious offenses.

Both the Strasbourg Convention 1990 adopted by the Council of Europe and the first money laundering directive adopted in 1991 by the European Commission required states to prohibit laundering proceeds of all serious crimes. Ten years after these instruments, the United Nations Convention against Transnational Organized Crime, 2000 (the Palermo Convention), which require countries to apply the offence of money laundering to the broadest range of predicate offences, was adopted.[99] Switzerland criminalized laundering property obtained from a felony (ie. a criminal offence punished with a prison sentence of more than three years[100]) in 1990.[101] At the time, any person who carried out an act that was aimed at frustrating the identification of the origin, the tracing or the forfeiture of assets which he knows or must assume originate from a felony was responsible for a money laundering offence.[102] English law criminalized laundering proceeds of all serious crimes with the Criminal Justice Act 1993. Laundering proceeds of drug trafficking and other serious crimes were prohibited by different acts before the adoption of the POCA 2002.[103]

---

[96] Recommendation 4, The Forty Recommendations of the Financial Action Task Force on Money Laundering 1990 <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf> 10 June 2021.

[97] R Fortson QC, 'Money laundering offences under POCA 2002' in W Blair, R Brent and T Grant (eds), *Banks and financial crime – the international law of tainted money* (2nd edn, OUP 2017), 136.

[98] Recommendation 5, FATF (n.96).

[99] Article 6 of the United Nations Convention against Transnational Organized Crime, 2000 (Palermo Convention).

[100] Article 10 (2), SCC 1937.

[101] Article 305*bis*, SCC 1937.

[102] Article 305bis of the Swiss Criminal Code as enacted

[103] Sections 49-53 of the Drug Trafficking Act 1994, sections 93A, 93B, 93C, 93D, 93H of Criminal Justice Act 1988 as amended by the Criminal Justice Act 1993 and sections 11, 12, 13, 17, 18A of the Prevention of Terrorism (Temporary Provisions) Act 1989. For further information see Annex B - The substantive UK law on money laundering in "Money Laundering Legislation: Guidance for Solicitors" (The Law Society, 14 August 2002) .

4.III.C. Definition of money laundering

Drage explained money laundering as follows: [104]

> Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If done successfully, it also allows them to maintain control over those proceeds, and ultimately to provide a legitimate cover for their source of income.

Similarly, Interpol defined money laundering as "any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources".[105] However, it is hard to adopt one single definition for money laundering because there are significantly different definitions adopted in diverse legal systems. It is worth mentioning that neither Drage's nor Interpol's definition fully complies with the FATF's recommendation 3.

4.III.D. Justifying punishment

4.III.D.1. The FATF recommendations

Punishing offenders is internally and externally instrumental toward the establishment of a society where everyone's rights and freedoms are respected.[106] Countries that are willing to create such a society are justified in punishing money launderers.

An offender attacks on the dispositional interest in the value of rights and freedoms by breaching another person's rights and freedoms.[107] By punishment, the State restores the victim's confidence in the value of his rights and freedoms.[108] Hence, punishment seeks to rectify a disturbance in the dispositional value of rights and freedoms.[109] Therefore, punishment is internally instrumental toward the establishment of a society where everyone's rights are respected. Furthermore, punishment is externally instrumental toward establishing a society where everyone's rights and freedoms are respected because it deters human agents or groups of human agents from acting in breach of others' rights.

---

[104] J Drage 'Countering money laundering: the response of the financial sector' (November 1992) B.E.Q.B. 2.
[105] "Money Laundering" (n3).
[106] Brown (n.13), 170.
[107] Ibid, 186.
[108] Ibid, 190.
[109] Ibid, 190.

The FATF's recommendation 3 advises countries to adopt punishment terms against two types of attacks on the dispositional interest in the value of rights and freedoms. First, the FATF recommends countries to punish one who pursues an act that aims to frustrate the practical application of confiscation rules on the assets he knows are or represent criminal property. In this scenario, the offender attacks on the dispositional interest in the value of rights by impeding the legal system's re-establishment of the dispositional equality of rights (eg. a professional money launderer who transfers criminal money to another country). Second, the FATF recommends countries to punish one who pursues an act on assets he knows are or represent criminal property while his act is not necessarily aimed at hiding the source origin of criminal assets (eg. mere acquisition, use or possession of the assets). In this case, the offender is not actively impeding the legal system's re-establishment of the equality of rights. However, the offender interferes with the victim's property rights by pursuing an act on assets knowing that he is acting without the property rights holder's consent. For instance, one who is using a stolen car breaches the car owner's property rights if he knows that the vehicle is stolen, even if he does not know who the real owner is. If the objective factual circumstances show that the alleged offender knows that the car is stolen, he is considered to have such information.

An agent who carries out an act to frustrate the practical application of confiscation rules or an agent who merely acquires, uses, possess etc. criminal property attacks on the dispositional interest in the value of victim's rights and freedoms. Punishment terms implemented on such agents are internally instrumental toward establishing a society where everyone's rights are respected because such terms aim to restore the victim's confidence in the value of his rights and freedoms.[110]

Punishment of money launderers is externally instrumental toward the establishment of a society where everyone's rights and freedoms are respected. First, punishment terms deter agents from acting in ways that frustrate the effective application of confiscation rules or acquiring, using, and possessing criminal property.[111] Second, by disturbing economic criminals, punishment may deter agents from committing economically motivated crimes.[112]

4.III.D.2 English and Swiss AML laws

The FATF recommends countries to criminalise money laundering on the basis of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (the Vienna Convention),[113] and the United Nations Convention against Transnational Organized Crime, 2000 (the

[110] Brown (n.13), 190.
[111] P He, 'A typological study on money laundering' (2010) 13(1) J.M.L.C. 15, 21-27.
[112] Becker (n.16), 88.
[113] Article 3(1) of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988, (Vienna Convention).

Palermo Convention)[114] and to apply this crime to all serious offences, with a view to including the widest range of predicate offences.[115] Sections 327, 328 and 329 in Part 7 of the Proceeds of Crime Act 2002 (POCA 2002) and article 305*bis* of the Swiss Criminal Code 1937 (SCC 1937) specify money laundering offences in the UK and Switzerland, respectively. English law is rated compliant with the requirements of the FATF's Recommendation 3,[116] while Swiss law is assessed 'largely compliant' with the relevant recommendation.[117]

Sections 327 to 329 of POCA 2002 criminalised two types of attacks on the dispositional interest in the value of rights and freedoms.[118] First, one may be prosecuted with a money laundering offence if he carries out an act that aims to frustrate the effective application of confiscation terms on the assets he knows or suspects is or represents criminal property without making an authorised disclosure. Second, one may be prosecuted with a money laundering offence if he pursues a prohibited act on assets he knows or suspects is or represents criminal property while his act is not necessarily aimed at hiding the source origin of criminal assets (eg. mere use or possession of the assets) without making an authorised disclosure. By adopting a remarkably low threshold, suspicion, English law went beyond the requirements of the FATF standards.

English AML laws, which adopted a remarkably low threshold, also established a new mechanism: the authorised reports regime. One does not commit a money laundering offence if he made an appropriate authorised disclosure, and where he made the disclosure before making the prohibited act, received appropriate consent from a competent public authority. Thus, one who does not know but suspects that some property is proceeds of crime and pursues a prohibited act on such property without making an authorised disclosure commits a money laundering offence.

One who accepts that he ought to act in compliance with his own and other persons' rights ought to take necessary measures not to act in breach of another agent's or other agents' rights. One who knows that his act X will breach another person A's rights, should decide not to do X unless he is ready to accept acting in breach A's rights. One who suspects that his act X may breach another person A's rights, he should take necessary and proportionate measures to ensure that his act X does not breach A's rights, unless he is ready to accept acting in breach A's rights .[119] English AML laws require one who must think that there is a possibility, which is more than fanciful, that his act may breach another person's rights to share its' suspicion with the competent public authorities.[120] One who fails to make such

[114] Article 6 of the United Nations Convention against Transnational Organized Crime, 2000 (Palermo Convention)..
[115] Recommendation 3, FATF (n.21), 12.
[116] FATF (n.29), 176.
[117] FATF (2016) (n.67), 160; and FATF (2020) (n.67), 11.
[118] Brown (n.13), 186.
[119] D. Beyleveld and R. Brownsword *Consent in the Law* (Oxford: Hart Publishing, 2007), Chapter 4.
[120] Sections 327-329 of POCA 2002, *R v Da Silva* [2006] EWCA Crim 1654 at [16].

disclosure takes the risk of acting in breach of another person's rights. He attacks on the dispositional value of rights by taking such risk.

The FATF's recommendation 3 advises countries to punish two types of attack on the dispositional interest in the value of rights, only the first one of which is accepted as a money laundering offence in Swiss law. According to article 305bis of SCC 1937, one commits a money laundering offence if he makes an act that aims to frustrate effective application of confiscation rules on the assets he knows or must assume is or represents criminal property.

4.IV. Banking industry and money launderers

The banking industry has largely been misused by economic criminals who wish to establish hard-to-detect money laundering schemes. This part shows the extent to which and the reason why money launderers misuse banking products and services. Moreover, it explores the reason why law enforcement agencies should follow the money found suspicious by the banks.

4.IV.A. The extent to which money launderers threaten the banking industry

More than 190 countries declared their aim to fight against money laundering,[121] while a successful global AML policy has not yet been achieved. Europol estimates that barely 1% of criminal proceeds in the EU are ultimately confiscated by relevant authorities,[122] while this ratio was estimated to be even lower at the global level.[123] According to the UNODC, "the estimated amount of money laundered globally in one year is 2 - 5% of global GDP."[124] Even the huge margin between those figures (3% of global GDP) reflects a significant weakness in the detection and, therefore, prevention and prosecution of economic crime.

Banking products and services have long and frequently been abused by criminals. It is submitted that a significant part of criminal money is being laundered by criminals using banking products and services.[125] Money launderers misused banking products and services so frequently that the banking

[121] See footnote 15 above.
[122] Europol, 'Does crime still pay? Criminal Asset Recovery in the EU - Survey of Statistical Information', European Police Office, 2016, 17.
[123] L de Koker and M Turkington 'Anti-Money Laundering measures and the effectiveness question' in B Rider (ed) *Research Handbook on International Financial Crime* (Edward Elgar Publishing 2015), 527.
[124] UNODC website, "Money – Laundering and Globalisation" <https://www.unodc.org/unodc/en/money-laundering/globalization.html> 10 June 2021.
[125] P Yeoh, 'Banks' vulnerabilities to money laundering activities' (2019) 23(1) J.M.L.C. 122, 122-135; Lombardini (n.68), 15; and F M Teichmann and B S Sergi, *Compliance in multinational corporations* (Emerald Publishing Limited 2018), 41. It is the banking industry that offenders misused in the 5 greatest money-laundering

industry appears to be the battleground between money launderers and law enforcement agencies. Most AML institutions were elaborated following erupted money laundering scandals where the offenders misused the banking industry. Indeed, banking scandals led to the adoption of general AML measures or AML measures that were initially specific to the financial sector, which then extended to other businesses fully or partly (eg. adoption of the CDD rules[126] and PEP regulations[127]). Hence, if money launderers and law enforcement agencies were chess players, the chessboard would have been the banking industry.

scandals (Wachovia Bank, Standard Chartered Bank, Danske Bank, Nauru banks and Bank of Credit and Commerce International cases).

[126] The 1977 scandal at the Chiasso branch of Crédit Suisse, which revealed that criminals had been taking advantage of the lack of regulation in banking business, leaded the Swiss Bankers Association to adopt the Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence 1977 (CDB 1977). Hence, the Swiss Bankers Association laid the foundation of customer due diligence regulations as a reaction to the Chiasso affair which caused inestimable damage to the reputation of the Zurich financial centre. (Capus (n90), 123.) 3 years after the CDB 1977, the Council of Europe recommended that banks should check the identity of new customers and make further checks where large sums of money were transferred. (Measures Against the Transfer and Safekeeping of Funds of Criminal Origin: Recommendation and Explanatory Memorandum, Council of Europe Rec No R (80) 10; for further details see W C Gilmore, *Dirty Money: the evolution of money laundering measures to counter money laundering and the financing of terrorism* (3rd edn, Council of Europe Press 2004), 161. This recommendation did not have a significant influence at least for a decade. (Ulph (n.92), 126.) Around 10 years after the 1977 scandal, the Pizza connection and Lebanon connection scandals, money laundering schemes which took advantage of banking services and products, were erupted. These cases speeded up Swiss legislator's criminalisation of both money laundering (article 305bis of the SCC) and insufficient diligence in financial transactions (paragraph 1 of article 305ter of the SCC). Hence, following a number of baking scandals, Swiss legislator elaborated CDD rules to be applied on financial institutions and criminalised insufficient diligence in financial transactions. The FATF, which was established in 1987, produced its' 40 recommendations in 1990, where it recommended countries to adopt customer identification and record-keeping rules to be applied on financial institutions. (Recommendation 12 – 20 of FATF (n.96).) In early 1990's, many countries adopted customer due diligence regulations to be applied in financial sector. (Ulph (n.92), 126.) In the wake of the 21st century, the scope of institutions which should undertake CDD measures have been extended and CDD measures became an important pillar of AML laws. Currently, the FATF recommends countries to adopt CDD measures to apply not only financial institutions but also designated non-financial businesses and professions. (FATF Recommendations 12 and 22.)

[127] Abacha affair which leaded adoption of PEP-specific AML rules shows the place of banking industry in the evolution of AML laws. It was argued that Sani Abacha, former dictator of Nigeria, as well as his family members and associates wrongfully appropriated several billion dollars from the Nigerian central bank and that the funds were transferred to bank accounts in a number of countries including the UK and Switzerland. (For further details, see E Monfrini, 'The Abacha case' in M Pieth (ed), *Recovering Stolen Assets* (Peter Lang AG 2008), 41-62. For a comparison of English and Swiss laws' reaction to Abacha affair, see Lombardini (n.68), 15.) The Nigerian government that succeeded the Abacha Regime in 1998 made an effort to recover the money and has been successful for more than 2 billion dollars. (Monfrini (n.127).) Abacha affair which affected many countries leaded emergence of the politically exposed person term. (Capus (n90), 125-126.) With its' resolution 55/61 of 4 December 2000, the United Nations General Assembly "established an ad hoc committee for the negotiation of an effective international legal instrument against corruption", after which the United Nations Convention against Corruption 2003 has been accepted. (United Nations Convention Against Corruption, 31 October 2003.) The same year, PEP specific rules to be applied financial institutions and designated non-financial businesses and professions entered into the FATF Recommendations. Recommendations 6-12, FATF (20 June 2003), 'The Forty Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf> 10 June 2021. and , for the current version see art. 12 and 22 and for the evolution process FATF (June 2013) 'FATF Guidance – Politically Exposed Persons (Recommendations 12 and 22)' <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf> 10 June 2021.

Ping He, in his typological study on money laundering, showed that money launderers are using banks in multitude ways.[128] In some cases, banking staff contribute to money laundering activities out of negligence, while in some others, they intentionally participate in the conspiracy. Moreover, several cases in the last 20 years have shown that powerful economic criminals do not only misuse banking products and services but also own banks to launder their tainted money.[129] For instance, charges announced by the US Department of Justice, on 20th November 2018, against three Venezuelan businessmen showed that these businessmen had bought a bank in the Dominican Republic in order to launder money and pay bribes.[130] Similarly, another recent case showed that the Antigua branch of the Austrian Meinl Bank AG was bought by Odebrecht S.A., a giant Brazilian construction company, to launder money and pay bribes.[131] As Maíra Martini from Transparency International puts it: "while buying a bank with the primary aim of using it to launder money seems something extreme, it is not the first time it has happened and probably won't be the last if supervision and control remain lax."[132]

By adopting Customer Due Diligence measures, lawmakers aimed at decreasing the number of banking staff contribute to money laundering activities out of negligence. Moreover, attributing banks a duty to report their suspicions may change their attitude from assisting their criminal clients to helping law enforcement authorities. Masciandro's research showed that the bankers decision to knowingly engage in money laundering practices is significantly affected by the penalty to the banks and their staff, in addition to the risk of the long-term loss of reputation.[133]

4.IV.B. The reason why the banking industry is threatened by money launderers

As a reaction to draconian confiscation measures explained in 4.II and penalties explained in 4.III and chapter 2, economic criminals started to develop sophisticated and hard-to-detect schemes "to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from

[128] P. He, (n.111), 19.
[129] M Martini, "Need help laundering money? What about buying your own bank?" Transparency Inernational Medium, 4 December 2018, < https://voices.transparency.org/need-help-laundering-money-what-about-buying-your-own-bank-5127457f09a8> 21 December 2018. M Levi, 'Money laundering and regulatory policies', in E U Savona, *Responding to money laundering – international perspectives* (Harwood academic publishers 1997), 263.
[130] "Venezuelan Billionaire News Network Owner, Former Venezuelan National Treasurer and Former Owner of Dominican Republic Bank Charged in Money Laundering Conspiracy Involving Over $1 Billion in Bribes", Department of Justice Office of Public Affairs, Justice News, 20 November 2018, <https://www.justice.gov/opa/pr/venezuelan-billionaire-news-network-owner-former-venezuelan-national-treasurer-and-former> 23 December 2018.
[131] Plea Agreement, United States of America against Odebrecht S.A. (Cr. No. 16-643 (RID)) <https://www.justice.gov/opa/press-release/file/919916/download> 19 December 2019.
[132] M. Martini, "Need help…" (n.129).
[133] F. Masciandaro, (1996) "Pecunia Olet? Microeconomia del Riciclaggio Bancario e Finanziario", Rivista Internazionale di Scienze Economiche e Commerciali, 43, pp. 817-844 via K Matthews, *Banks and the laundering of dirty money: The economics of money laundering* (Cardiff University, Discussion papers in Economics, August 2000), 17.

legitimate sources".[134] Money launderers threaten the banking industry because the banking industry can provide economic criminals with what they need to develop hard-to-detect money laundering schemes.

4.IV.B.1. What do economic criminals need?

According to the basic framework of Becker,

> there is a function relating the number of offences by any person to his probability of conviction, to his punishment if convicted, and the other variables, such as the income available to him in legal and other illegal activities, the frequency of nuisance arrests, and his willingness to commit an act.[135]

Confiscation terms may deprive the offenders of the proceeds of crime. Moreover, those who launder proceeds of crime may face serious punishment. Therefore, economically motivated offenders should either stop committing a crime or find a way to escape from law enforcement authorities' radars.[136]

To escape from AML laws, both economically motivated offenders and other economic criminals should use their illicit wealth in a manner in which law enforcement authorities cannot detect. If an offender uses illegal money for his daily needs (eg. a pickpocket who spends the money for grocery shopping), the tainted money is unlikely to be detected by law enforcement authorities.[137] However, those economic criminals who make a handsome sum of money from their criminal business such as drug and gun dealers, as well as criminal organisations often have a considerable amount of extra money that they do not spend for their living or their illegal business.[138]

Money that is not used by the offender is less likely to be found by police.[139] Accordingly, one way of hiding from police authorities is hiding criminal money, keeping it away from the legal economy. However, hiding money comes with significant disadvantages. First, hidden money is vulnerable to theft and physical damage. Roberto Escobar, the chief accountant and brother of Pablo Escobar, known as the 'king of cocaine', tells in his book that "Pablo was earning so much that each year we would write off 10% of the money because the rats would eat it in storage or it would be damaged by water or lost".[140] Storing precious metals (eg. gold and silver) or high denomination banknotes (eg. 500 Euro

---

[134] "Money Laundering" (n3).
[135] Becker (n.16), 88.
[136] In relation to the economically motivated offenders' willingness to commit economic crime, see Kranacher et all. (n.90), 86.
[137] M M Gallant, *Money laundering and the proceeds of crime – Economic crime and civil remedies*, (Edward Elgar 2005), 2.
[138] See 'predators' in Kranacher et all. (n.90), 87-89.
[139] Gallant (n.137), 2.
[140] R Escobar and D Fisher, *The Accountant's Story: Inside the violent world of the Medellín cartel* (Grand Central Publishing 2009), 114.

banknotes which have now been phased out over fears of links to organised crime,[141] and 1000 Swiss Franc banknotes[142]) seems helpful to offenders. However, it is worth mentioning that offenders often obtain money in small banknotes and businesses by which they may buy precious metals or exchange money are regulated for fighting against money laundering.[143] Second, economic criminals face an opportunity cost because they cannot use hidden money for investment. In fact, economic criminals cannot even spend their illegal money to buy luxury products if they wish to hide the money from law enforcement agencies since luxury spending may call law enforcement authorities' attention. The reports list many cases where offenders with low or medium legal income were caught by the law enforcement authorities after making luxury spending (eg. buying expensive boats, cars or jewellery).[144] Lastly, even hidden money is, to some extent, vulnerable to detection.[145] For instance, noise from a money-counting machine in Franklin Jurado's house, which prompted a neighbour to alert the local police, was one reason why Luxembourg police started an investigation on the famous money launderer.[146] All in all, an economic criminal who hides illegal money is similar to an axe thief who hides the axe he had stolen and never uses it.

Another way of using illegal money without disruption may be using it after cleansing its' illegal source origin. By laundering criminal money, the offender hides the illicit source origin of money, not money itself. This may be seen as a more sophisticated version of a method used by an axe thief who reshapes the stolen axe so that he can use it with no disruption. Laundering illegal money is more profitable for economic criminals. Indeed, once it has been laundered, the offender can use the illicit money as he wishes to. However, laundering proceeds of crime comes with its own problems. First, money laundering is recognised as a separate criminal offence. Second, laundered money is also subject to confiscation. Therefore, money launderers need to establish undetectable money laundering schemes to cleanse illicit money.

---

[141] Europol Report, 'From suspicion to action: Converting financial intelligence into greater operational impact' (2017), 22 <https://www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact> 1 June 2021.

[142] Use of 1000 Franc banknotes has been subject to a vivid debate since 500 Euros banknotes were phased out over fears of links to organised crime. For instance, 13.4258 - Interpellation, 'Pourquoi y-a-t-il tant de coupures de 1000 francs en circulation depuis 2008?' <https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20134258> 1 June 2021 ; and 16.3114 – Interpellation, 'Engouement pour les billets de 1000 francs. La réputation de la Suisse est-elle en danger?' <https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163114>.

[143] The FATF recognised money remittance and foreign currency exchange businesses as a subset of financial institutions. (FATF (n,21) 120.) For a further investigation of AML measures to be applied in these businesses, see FATF (June 2010), 'FATF Report: Money Laundering through Money Remittance and Currency Exchange Providers' <https://rm.coe.int/fatf-report-money-laundering-through-money-remittance-and-currency-exc/16807150ad> 1 June 2021. Moreover, the FATF recognised dealers in precious metals and dealers in precious stones as a subset of designated non-financial businesses and professions. (FATF Recommendation 22).

[144] FATF, 'Money Laundering and Terrorism Financing 2004-2005 Typologies' Financial Action Task Force, Paris, 10 June 2005.

[145] P. He, (n.111), 20.

[146] "Special Future- Money Laundering" (n.88). For another case where illegal money that was stored in an apartment was detected by police authorities TF, 14 aout 2002, 6S.702/2000 and 20 mai 2009, 6B_1021/2008.

While it is hard, if not impossible, to argue that a laundering structure is undetectable, three factors can significantly contribute to its' success. First, adding international transactions makes a money-laundering scheme more successful.[147] International transactions are harder for law enforcement authorities to follow due to some communication and cooperation problems between foreign law enforcement authorities (eg. language barrier, privacy laws). After the Danske Bank Estonia scandal in 2017, Tom Keatinge, the director of the Centre for financial crime and security studies at the Royal United Services Institute, put it that: "The borders are immaterial to you when you are structuring … [illicit] transactions, whereas the borders are not immaterial for the cops who are trying to chase you."[148]

Second, buying information from insiders may handsomely contribute to the undetectable nature of a laundering scheme. Corrupted officers can help criminals stay one step ahead of law enforcement authorities by providing them with insider information. The City of London police is argued to estimate that 35% of its' cases involve some insider element.[149] This is the reason why law enforcement agencies see a successful fight against corruption as a prerequisite to an effective fight against money laundering.[150]

Third, talented financial and legal experts may assist launderers in setting up hard to detect laundering schemes. For instance, Colombian drug lord Jose Santacruz-Londono had been cleansing his illegal money in the late 1980s and early 1990s with a famously elaborate money-laundering scheme created by a Harvard-educated economist.[151] This was stressed out in a UN note as follow: [152]

> Using the tools he learned at America's top university, *[Franklin Jurado]* moved $36 million in profits, from US cocaine sales for the late Colombian drug lord Jose Santacruz-Londono, in and out of banks and companies in an effort to make the assets appear to be of legitimate origin… The Jurado case is an example of the increasingly sophisticated means drug cartels employ to secure assets.

Forth, establishing a "keep your mouth shut culture" amongst those involved in the criminal conspiracy is essential for the offenders to reach their aim of cleansing illicit money.[153] It is only by creating a

[147] Kranacher et all. (n.90), 101.
[148] J Garside, "Is money-laundering scandal at Danske Bank the largest in history?" The Guardian, 21 September 2018, <https://www.theguardian.com/business/2018/sep/21/is-money-laundering-scandal-at-danske-bank-the-largest-in-history> 13 October 2018.
[149] "Lloyds TSB on the trail of insider fraud" *The Financial Times,* 6 June 2007. Via F Hobson, 'Introduction: Banks and Money Laundering' in W Blair and R Brent (eds), *Banks and Financial Crime: The International Law of Tainted Money* (OUP 2008) 15.
[150] Muller (n.87), 9; Rapport du groupe interdépartemental de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme (GCBF), "National Risk Assessment (NRA) : La corruption comme infraction préalable au blanchiment d'argent", Avril 2019, 9 <https://www.cdbf.ch/wp-content/uploads/2019/07/20190710_ber-korruption-geldwaescherei-f_final1.pdf> 1 June 2021.
[151] "Special Future- Money Laundering" (n.88).
[152] Ibid.
[153] In relation to keep your mouth shut culture and how this may effectively obstruct justice, see Chicago Inspector General Joe Ferguson, video in <https://news.wttw.com/2019/01/30/inspector-general-decries-keep-your-mouth-shut-culture-city-hall> 10 June 2021.

strong secrecy culture money launderers can stop whistle-blowers. Hence, money launderers should benefit from insiders and find a way to impede the inverse.

Hiring insiders and experts as well as buying their silence requires substantial financial and political power. Economic crime, arguably the third biggest industry worldwide, enable some offenders to obtain such financial and political power.[154] Committing economic crime and laundering proceeds of crime constitute handsomely profitable businesses, and economic criminals, particularly criminal organisations involved in economic crimes and money laundering, control a strong financial power.[155] This financial power enables them to obtain a robust political power too.[156] Indeed, there are many cases where criminals were proven to have established strong connections with high-level officials and gained political power. For instance, in 2017 Odebrecht S.A. case, the giant Brazilian construction company, was proven to have bought and used Antigua branch of the Austrian Meinl Bank AG for laundering money and paying bribe to officials. Odebrecht S.A. is said to have "funded plots to elect a half-dozen presidents in Latin America; buy the friendship of heads of state in Angola, Peru, and Venezuela; and pay off hundreds of legislators from Panama to Argentina".[157] Odebrecht's plea agreement with the United States, Brazilian and Swiss authorities highlighted that, "[B]y virtue of this acquisition, other members of the conspiracy, including senior politicians from multiple countries receiving bribe payments, could open bank accounts and receive transfers without the risk of raising attention."[158] Crime groups establish sophisticated mechanisms to pay bribes to corrupted officials and may have the power to eliminate non-corrupted ones. Muller argues that the murder of the Vice president of the Russian Central Bank, Mr Andrey Kozlov, responsible for the supervision of banks, on 14 September 2006 indicate frightening powers of international criminal organisations involved in money laundering and terrorist financing.[159] It is worth noting that the Russian Interior Ministry had estimated, some 7 years before the murder of Mr Andrey Kozlov, in 1999, that crime syndicates control half of Russia's banks.[160] Hence, economic crimes are so profitable that money laundering became a sophisticated

[154]A V M Leong, 'Anti-money laundering measures in the United Kingdom: a review of recent legislation and FSA's risk-based approach' (2007) 28(2) Co Law 35, 40.

[155] According to the United Nations Office on Drugs and Crime, "the estimated amount of money laundered globally in one year is 2 - 5% of global GDP" UNODC (n.124), while the European Commission's 2013 impact assessment of the EU AML/CTF legislative framework indicates that "global criminal proceeds potentially [amount] to some 3.6% of GDP; around US$2.1 trillion in 2009". Footnote 1 from HM Treasury and Home Office (UK), 'UK National Risk Assessment of Money Laundering and Terrorist Financing', October 2015, reads as follow: '"Impact Assessment accompanying the document proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering, including terrorist financing and Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds", European Commission, Feb 2013'

[156] M. Martini, "Need help…" (n.129);

[157] M Smith, S Valle and B. Schmidt, 'No One Has Ever Made a Corruption Machine Like This One' Bloomberg Businessweek, 8 June 2017, <https://www.bloomberg.com/news/features/2017-06-08/no-one-has-ever-made-a-corruption-machine-like-this-one> 30 June 2021.

[158] Plea Agreement (n.131).

[159] Muller (n.87), 9.

[160] Economist (1999), "Russian Organised Crime", *The Economist* Aug 28th – Sept. 3rd 1999, 18 via Matthews (n.133), 8

international organised crime, conducted by wealthy and politically influential crime groups that employ insiders and qualified financial and legal experts. However, this is by no means that the offence of money laundering is committed by these powerful groups only.

4.IV.B.2. What can the banking industry offer money launderers?

The banking industry has largely been targeted by money launderers, because it may provide offenders with what they need. First, banking institutions offer many products and services that economic criminals may use in different stages of money laundering. Second, banking staff involve financial and legal experts who work within a strong confidentiality culture, who may assist offenders.

4.IV.B.2.a. Banking institutions provide financial products and services needed by money launderers

Money laundering consists of 3 stages: placement, layering and integration. Products and services provided by financial institutions (eg. deposit, loan, acceptance, foreign exchange, settlement, financial transfers and the like) can be of use to criminals for each of these stages. Moreover, banking services and products may help offenders adding an international dimension to their money laundering scheme.

In the first stage, the money launderer aims to place illegally obtained money, usually in cash form, into the legal economy. This may be achieved in many different ways such as depositing money into a bank account, buying real estate, or starting a business.[161] However, one who directly deposits high sums of money into the legal economy (eg. one who purchases real estate), may attract law enforcement authorities' attention. Therefore, criminals often place high sums of illicit money by using multiple individuals (ie. smurfing method) and multiple transactions (ie. structuring method).[162] Law enforcement authorities are unlikely to detect any suspicious activity where each transaction and person deposits an insignificant sum of money.[163] For instance, according to a typology report by Masak, Turkey's FIU, a financial controller noticed in 1996 that 29 million US dollars had been placed into the financial system and consequently transferred abroad with more than 48.000 transactions, none of which was higher than 600 dollars.[164]

[161] Teichmann and Sergi (n.125), 34-35.
[162] Teichmann and Sergi (n.125), 38.
[163] Teichmann and Sergi (n.125), 109.
[164] Masak website, Örnek davalar available <http://www.masak.gov.tr/tr/content/aklama-yontemleri/59> 10 June 2021.

Because banking institutions provide multiple products and services that facilitate depositing cash into the financial system, money launderers can benefit from the banking products and services in the placement stage. Banking products and services have two advantages for criminals in the placement stage. First, the clients can split cash deposits into smaller amounts because it is easy to employ smurfing and structuring methods within the banking industry. Criminals may deposit money into their accounts in different banks in multiple times (structuring).[165] Moreover, money launderers can employ money mules, such as students, to place criminal money (smurfing).[166] Second, banking clients can abstain from the service providers' direct questions, since some banking services give clients a chance to deposit money without a face-to-face inquiry by any human being. For instance, bank clients can deposit small amounts of cash by using ATMs, while business customers can use night safes to deposit a higher amount of money avoiding face to face inquiries by bank employees.[167]

To impede law enforcement authorities from tracking the lien between the money placed into the financial system and its' illegal source origin, a layering stage, which should consist of multiple national and international, direct and indirect financial transactions, follows the placement stage.[168] This stage is to separate money and its' illegal source origin. For instance, in Franklin Jurado's famous laundering structure, money was shifted between more than 100 accounts in 68 banks in 9 countries.[169]

In the last stage, the integration stage, illicit money, which gained a seemingly legal source origin, is integrated into the offender's wealth. The integration stage represents the final step of the layering stage. However, because the end user's identity may be beneficial for the law enforcement authorities, the integration stage is of particular importance for both criminals and police.[170]

Because banks provide secure, fast and low-cost national and international financial transaction services,[171] they are frequently used by economic criminals in layering and integration stages. Besides, banks offer some products and services which may facilitate indirect transfers. While banking services which provide indirect transactions are relatively more expensive and time-consuming, they play an

[165] Teichmann and Sergi (n.125), 38.
[166] F Keating, "Gangs force thousands of teens to become 'money mules'", Independent, 29 July 2017 <https://www.independent.co.uk/news/uk/teenagers-money-laundering-money-mules-criminal-gangs-gangsters-criminals-fraud-a7866151.html> 10 June 2021.
[167] For a case reported by the Egmont Group reported where the offender deposited his illegal money - the majority in old bills- into the bank's night safe to avoid difficult face-to-face questions, see *FIU's In Action – 100 Cases from the Egmont Group* (Weimin 2005), 173 (Case 15).
[168] S Savla, *Money Laundering and Financial Intermediaries* (Kluwer Law International 2001), 8.
[169] "Special Future- Money Laundering" (n.88).
[170] J Biggins, 'Dirty complexity: money laundering through derivatives' in B Unger and D van der Linde (eds) *Research Handbook on Money Laundering* (Edward Elgar Publishing 2013), 324.
[171] S Ogilvie and S Revell, 'International Anti-Money Laundering Initiatives' in G Godfrey and F Neate (eds), *Neate and Godfrey: Bank Confidentiality* (Bloomsbury Professional 2015), 1004.

essential role in hiding the source origin of illicit money.[172] Loan back schemes may constitute an important example of indirect transactions. Matthews explains loan back schemes as follows:[173]

> The launderer transfers the illegal cash to another country, (usually by currency smuggling) and then deposits the proceeds as security for a bank loan, which is credited back to the original country. The remittance of the laundered cash in the form of a loan has the appearance of a legitimate international loan with the potential for a reduction in tax liability.

In the Pizza Connection Trial, it was detected that drug money gained by the Sicilian mafia in the US was smuggled to Switzerland and deposited to Swiss banks in the names of Swiss shell companies. This money was used as security for bank loans credited from Paris and London banks to New York Pizzeria.[174]

To summarise, banking institutions are frequently misused by money launderers, because the former provide multiple products and services that the latter needs.

4.IV.B.*2*.b. Banking staff involve financial and legal experts who work with a strong confidentiality culture

Banking staff involve financial and legal experts who can provide criminals with both expert and insider support. In particular, they can assist their criminal customers by informing them about financial transactions that are likely to draw law enforcement authorities' attention. This is because banking staff may have substantial knowledge on the capacity and methods of relevant law enforcement authorities due to the cooperation between them and law enforcement authorities.

On the one hand, banking staff can provide money launderers with expert and insider support. On the other hand, law enforcement authorities can detect money laundering schemes thanks to the information provided by banking staff. For instance, the ongoing Danske Bank Estonia investigation, where the bank is argued to act as the hub of a $234bn money-laundering scheme, was initiated by the information revealed by a whistle-blower, who was later identified as a former employee of the bank.[175] Hence, money launderers who benefit from banking staff need a keep your mouth shut culture to protect themselves. In establishing that, the strong secrecy culture in the banking business may help them.

---

[172] Lombardini (n.68), 89.
[173] Matthews (n.133), 10.
[174] Matthews (n.133), 10. Similar examples may be found in TPF, 10 octobre 2008, SK.2007.24, cons. 3.1; TF, 22 avril 2005, 1S.13/2005; and TF,12 mai 2006, 1P.81/2006.
[175] 'Howard Wilkinson', National Whistleblower Center, <https://www.whistleblowers.org/members/howard-wilkinson/> 10 June 2021; and F Coppola, 'The Banks That Helped Danske Bank Estonia Launder Russian Money', Forbes, Sep 30, 2018, <https://www.forbes.com/sites/francescoppola/2018/09/30/the-banks-that-helped-danske-bank-estonia-launder-russian-money/#3defa2207319> 10 June 2021

Secrecy culture in the banking business is stronger than the one in many other businesses, making banking business a better choice for criminals.[176]

Secrecy culture in the banking business is older and stronger than the one in many other businesses[177] because economic reasons oblige banks to respect their clients' secrecy.[178] Financial centres and financial institutions can increase their attractiveness by adopting and following strong secrecy rules. Conversely, they can lose existing or prospective clients where they fail to respect their clients' financial secrecy. Some financial centres owe their attractiveness to their famously strong bank secrecy laws. For instance, Switzerland has long had famously strong financial secrecy laws and its' famous secrecy laws handsomely helped Switzerland to become an attractive financial centre.[179] Moreover, because financial secrecy has an economic value for financial institutions, bankers share an ancient and strong culture of secrecy even in countries that are not famous for their bank secrecy laws. For instance, English bankers had been protecting their clients' secrecy way before English law recognised bankers' legal duty of secrecy.[180]

4.IV.C Follow the money approach and the STRs/SARs produced by banks

Law enforcement authorities can identify unrevealed economic crime by following suspicious money. The FATF notes that "[t]he link between the origins of the money, beneficiaries, when the money is received and where it is stored or deposited can provide information about and proof of criminal activity".[181] In fact, often an economic crime

> is not identified immediately through the recognition of the conduct, but as a consequence of identifying funds that move within the financial markets, through the accumulation of unexplained wealth, the sudden collapse of an individual investment scheme, or simply the purchase of expensive goods or services.[182]

Money laundering typology reports demonstrate many examples where law enforcement authorities identified economic crime following suspicious money.[183] Therefore, countries willing to fight against

[176] Mary Alice Young, *Banking secrecy and offshore financial centers: Money laundering and offshore banking* (Routledge 2013), 27.
[177] See pages 37-39 and 64-66 in chapter 2.
[178] See pages 64-66 in chapter 2.
[179] See pages 64-66.
[180] See pages 37-39.
[181] FATF, 'Operational Issues Financial Investigations Guidance', June 2012, 3.
[182] K McCarthy, 'UK Part I: Laundering the proceeds of crime – Methodology?' in M Simpson, N Smith and A Srivastava (eds), *International guide to money laundering law and practice* (3rd edn, Bloomsbury Professional 2010) 1.
[183] A long list of examples may be found in FIU's In Action (n.167); and FATF (n.144).

economic crime and criminal money should adopt a follow-the-money approach, and follow the suspicious money.

To detect suspicious money, law enforcement agencies need accurate and adequate financial information.[184] Financial institutions obtain and observe valuable financial information relating to their customers (eg. financial transaction data). Therefore, lawmakers took measures to increase law enforcement agencies' capacity to obtain information from financial institutions. First, they were given the power to request information from financial institutions.[185] However**,** they cannot obtain all banking data due to some technical constraints as well as privacy and confidentiality concerns. Therefore, lawmakers made effort to create a system where financial institutions share their suspicions with law enforcement agencies.

Law enforcement agencies should follow transactions and activities that bankers find suspicious due to two reasons. First, they should control the banking industry carefully, because the banking industry is seriously threatened by economic criminals. Countries should identify, assess, and understand the money laundering risks for the country, and should apply a risk-based approach to ensure that measures to prevent or mitigate money laundering are commensurate with the risks identified.[186] As explained above, banking is a high-risk business. The general principle of a risk-based approach is that, "where there are higher risks, relevant persons should take enhanced measures to manage and mitigate those risks".[187] Accordingly, countries should take enhanced measures to apply banking industry, one of which is following suspicious banking transactions. Second, law enforcement agencies should take bankers suspicion seriously because bankers have the expertise and financial data that enables them to distinguish their client's regular, unusual and suspicious activities.

As explained above, bankers involve financial and legal experts who can distinguish their client's regular, unusual and suspicious financial transactions.[188] It is worth noting that AML laws require banks

---

[184] R Parlour, 'Practicalities of Financial Crime Deterrence' in B Rider (ed), *Research Handbook on International Financial Crime* (Edward Elgar Publishing 2015), 305; A Bacarese, K Levy and H Mulukutla, 'The management of information in the context of suspected money laundering cases' in B Rider (ed), *Research Handbook on International Financial Crime* (Edward Elgar Publishing 2015), 513.

[185] Recommendation 31, FATF (n.21), 25; In relation to English law enforcement authorities' power to take additional monitoring measures if the property is related to a ML or TF offence, see Part 8 of POCA; POCA 2002 (References to Financial Investigators) (England and Wales) Order 2015; POCA 2002 (References to Financial Investigators) (Amendment) Order 2009; Part II and III of Terrorism Act 2000, section 29 of Regulation of Investigatory Powers Act 2000; sections 19,102 and 103 of Investigatory Powers Act 2016; section 93 of Police Act 1997 as well as section 7 of Crime and Courts Act 2013. See INR 31, FATF (n.29), 226. See also J Peddie, 'Investigations and remedies under POCA 2002', in W Blair, R Brent and T Grant (eds), *Banks and financial crime – the international law of tainted money* (2nd Edition, OUP 2017), [19.01]-[19.07].
In relation to Swiss law enforcement authorities' power to take additional monitoring measures if the property is related to an ML or TF offence, see chapter 4 of Swiss Criminal Procedure Code 2007, in particular articles 246, 269, 280, 285a and 298a. For further information see: INR 31; FATF (2016) (n.67), 215.

[186] Recommendation 1, FATF (n.21), 10.

[187] Interpretive Note to Recommendation 1, FATF (n.21), 31.

[188] See 4.IV.B above.

to provide their clients with AML training. The FATF underlined that Financial institutions' programmes against money laundering should include an ongoing employee training programme.[189]

Data in possession of banks relating to their customers can play an essential role in the fight against money laundering. Due to their close professional connection with their clients, banks acquire and observe a wide range of information that may help them identify the client's real purpose in using banking services. Money launderers often carry out transactions that are not normal to their profile. For instance, the offender may place money into the financial system more than what is expected to his financial profile, the offender may place old bills, high nomination bills or foreign currency bills more frequently or in higher value than what is expected to his financial profile, the offender may be making frequent or high-value international transactions than what is expected.[190] Criminal clients' unusual and suspicious activities may naturally be seen in the records of the banks.[191] An investigator quoted in the Kerry Report had underlined the importance of banking data as follow:

> [Bank of Credit and Commerce International] had 3,000 criminal customers and everyone of those 3,000 criminal customers is a page 1 story. So if you pick up anyone of accounts … you will find all manner and means of crime around the world in the records of this bank.[192]

Moreover, banks are required to undertake customer due diligence measures that help them know their clients.[193] Therefore, data scientists argue that the success of AML policies in the current banking industry depends on the adequacy and quality of banking data.[194]

To summarise, law enforcement agencies should take bankers' suspicion seriously, because bankers are experts who can distinguish regular, unusual and suspicious transactions of their clients and they have access to personal, private and confidential information that is valuable to distinguish regular, unusual and suspicious transactions.

[189] Interpretive Note to Recommendation 18, FATF (n.21), 85.
[190] Europol (n.141) 22.
[191] M Harari, «Procédure pénale : la banque comme détentrice d'informations et de valeurs patrimoniales appartenant a son client» in L Thevenoz, C Bovet (eds), *Journée 2010 de droit bancaire et financier*, 95.
[192] An investigator quoted in the Kerry Report. Kerry Report, 1992, vol 1, p. 61.
[193] See pages 24-28 in chapter 2.
[194] J Thomas, 'Money laundering in the 21st century: Follow the money' Payments Cards & Mobile website <http://www.paymentscardsandmobile.com/money-laundering-in-the-21st-century/> 9 June 2021.

CHAPTER 5: ANTI-MONEY LAUNDERING LAWS IN BREACH OF DATA PRIVACY STANDARDS AND THE SUCCESS OF THE SUSPICIOUS TRANSACTION REPORTS REGIME

5.I. Introduction

This chapter defends that AML laws in breach of information privacy standards decrease countries' success in the fight against economic crime, criminal money, and money laundering.

Chapter 3 showed that Anti-Money Laundering (AML) laws requiring and permitting banks to make Suspicious Transaction Reports (STRs) restrict banking clients' information privacy rights. Information privacy laws do not establish an absolute duty of secrecy. Lawmakers can legitimately restrict banking clients' information privacy rights if the following three conditions are met: (i) the restriction is in accordance with the law, (i) the restriction pursues a legitimate aim, (iii) and the restriction constitutes a necessary and proportionate measure to achieve the legitimate aim pursued. Hence, AML laws requiring and permitting banks to make STRs can legitimately interfere with banking clients' information privacy rights if they meet listed conditions.

Restriction of banking clients' information privacy rights should be in accordance with the law and the law must be clear, foreseeable, and accessible. English and Swiss lawmakers restricted banking clients' information privacy rights in accordance with the law.

AML laws requiring and permitting banks to make STRs pursue a legitimate aim, that is the detection, prevention and prosecution of crime. Chapter 4 defended that establishing an STRs regime that applies to banks is essential to fight against economic crime, criminal money and money laundering.[1] Therefore, bankers should be required and permitted to report their client's suspicious transactions by making STRs.

Lastly, the restriction should be necessary and proportionate to achieve the legitimate aim pursued. This chapter defends that English and Swiss law-makers failed to specify proportionate measures, leading bankers to make unwarranted reports. Unwarranted reports not only breach reported person's information privacy rights[2] but also reduce the success in the fight against economic crime, criminal money, and money laundering.

[1] See pages 159-161 in Chapter 4.

[2] There is an unjustified interference with the reported banking client's privacy rights where a report is unnecessarily made, even if it has no substantive effect on the banking client. The European Court of Human

The FATF took a big step in February 2018 integrating data protection and privacy laws into its recommendation 2. To increase the success in the fight against economic crime, criminal money and money laundering, the FATF should take further steps to underline the importance of data protection and privacy laws.

5.II. Compatibility of AML laws with data protection and privacy rules and the success of the STRs regime

AML laws in breach of information privacy standards often lead bankers to make low-quality disclosures (ie. unwarranted or poorly justified disclosures). Low-quality reports breach banking clients' information privacy rights and hamper the effectiveness of the STRs regime.

5.II.A AML rules in breach of information privacy standards lead bankers to make low-quality disclosures.

AML laws made banks the policemen of the financial sphere.[3] Whilst, banks are profit-oriented private entities. Their profit-oriented actions may hamper the effectiveness of AML institutions. For instance, banks are expected to undertake enhanced customer due diligence measures where their client belongs to a high-risk category.[4] However, it is submitted that many banks prefer terminating business relationships with those clients to avoid, rather than manage money laundering risk.[5] De-risking or de-banking leads to unjustifiable financial exclusion of some categories of people (eg. immigrants), and financial exclusion decreases countries' success in the fight against economic crime.[6] This chapter defends that the STRs regime related AML rules that are in breach of information privacy standards often lead bankers to make low-quality disclosures.

Rights established, in *Sommer v Germany* (2018) 67 E.H.R.R. 9, that "collecting, storing and making available the applicant's professional bank transactions constituted an interference with his right to respect for professional confidentiality and his private life." For further discussion, see pages 115-118 in chapter 3.

[3] See pages 19-28 in chapter 2.

[4] See pages 21-23 in chapter 2.

[5] A number of examples may be found in M Akgun, 'Turkey – financial institutions' anti-money laundering/counter-terrorist financing duties and financial exclusion' (April 2021) PL 445, 446; T Durner and L Shetret, 'Understanding bank de-risking and its effects on financial Inclusion (London: Oxfam 2015), 9-23; L Isaacs et al, 'Impact of the Regulatory Environment on Refugees' and Asylum Seekers' Ability to Use Formal Remittance Channels', July 2018, Knomad Working Paper 33, 21-23 <https://www.knomad.org/sites/default/files/2018-07/KNOMAD_WP_Impacts%20of%20the%20Regulatory%20Environment%20on%20Refugees%e2%80%99%20and%20Asylum%20Seekers%e2%80%99%20Ability%20to%20Use%20Formal%20Remittance%20Channels.pdf> 10 June 2021.

[6] Durner and Shetret (n,5), 18; Akgun (n,5), 446.

A banker who detected an unusual transaction has three choices. First, he may decide to investigate the issue further in order to determine whether it is worth reporting. Second, he may continue providing service to the client with unusual transactions without making an STR or further investigating the issue. Third, he may make an STR out of caution, even if he does not genuinely suspect that the client's funds constitute or represent illicit money.

In an STRs regime, the bankers are expected to report their client's suspicious transactions, not all unusual transactions. The Joint Money Laundering Steering Group Guidance explains the difference between unusual and suspicious transactions as follows:[7]

> A transaction which appears unusual is not necessarily suspicious. Even customers with a stable and predictable transactions profile will have periodic transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of transactions or account activity. So the unusual is, in the first instance, only a basis for further enquiry, which may in turn require judgement as to whether it is suspicious.

Bankers often face unusual transactions. They are required to examine their client's unusual transactions to determine whether such transactions are worth reporting.[8] If the transaction is suspicious, the banker is expected to file a report with the Financial Intelligence Unit (FIU). If the unusual transaction examined is not assessed suspicious, the bank should not make an STR.

The above-explained course of action (ie. examining the unusual transactions and reporting only suspicious transactions) enables bankers to comply with both AML laws and information privacy laws. However, further investigating the issue costs time and money.[9] AML compliance costs billions of dollars to financial institutions across the world and banks are profit-oriented entities wishing to minimise expenses.[10]

Option two is remaining unresponsive to the unusual transaction (ie. not making an STR, not undertaking a further examination of the unusual transaction and keep providing service to the client with unusual transactions). Several reasons may lead bankers to choose this course of action. First, the banker may be working in a bank that does not have enough staff members or an AML system to analyse each unusual transaction. Second, the banker may be working in a bank that does not provide AML training to its staff members. Third, the banker may be involved in a criminal conspiracy. However, it

---

[7] JMLSG, Prevention of Money Laundering, 2009, [6.12].

[8] See The FATF's Recommendation 10(2)-iii, FATF (2012-2020), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, 14, <www.fatf-gafi.org/recommendations.html> 10 June 2021; Article 27(2)(c) of UK's Anti-Money Laundering Regulations 2017; and Article 6(2) of Switzerland's Anti-Money Laundering Act 1997. See pages 25-27 in chapter 2.

[9] M Yeandle et al, *Anti-Money Laundering Requirements : Costs , Benefits And Perceptions* (Z/Yen 2005), 24.

[10] LexisNexis Risk Solutions Survey 2017 found that the true cost of AML/CTF compliance to financial institutions across the 5 European Markets, namely Switzerland, France, Germany, Italy, and the Netherlands, was US$83.5 billion annually. 'The True Cost of Anti-Money Laundering Compliance -Survey Report, September 2017, LexisNexis Risk Solutions, 4.

is worth noting that non-reporting banking staff and/or the bank may face criminal, administrative and regulatory sanctions for failure to report.[11]

The third option is reporting all unusual transactions. A banker facing an unusual transaction may file an STR with the FIU out of caution while he does not genuinely suspect that the client's funds constitute or represent criminal money. By making an STR, the reporting person protects himself and the bank for which he is working from acting in breach of AML laws. However, one who makes an unwarranted disclosure breaches the reported client's information privacy rights. Furthermore, the bank may lose its attractiveness if people learn that that bank is making unwarranted disclosures.

There may be several factors leading bankers to make low-quality disclosures. First, if the failure to report is specified as a serious criminal offence, bankers may be inclined to make unwarranted defensive reports. Second, if AML laws are ambiguous and unforeseeable to the extent that banking staff fail to understand what they are expected to report, they may make reports out of caution. Third, if the reporting persons' legal and financial interests are overly protected by law, making an STR without further investigating the unusual transaction may be a cost-effective strategy. Therefore, AML laws that overly protect the reporting person's legal and financial interests may lead bankers to choose the third option.

5.II.B Low-quality reports and the effectiveness of the STRs regime

The FATF, in its' recommendations released in 1990, advised countries to create a mandatory or voluntary STRs regime that applies to banks and non-bank financial institutions.[12] Establishing a system where banks report suspicious transactions of their own clients was a surprising and challenging objective at the time. When Wadsley defended in 1994 that AML laws made banks the private policemen of the financial sphere, she was spelling out a fact that was shocking to the majority of banking professionals.[13] Voluntary STRs regimes showed that the bankers were not disposed to report their clients' suspicious activities.[14]

It has been more than 30 years since the FATF's recommendations 1990 were released. Some banking officials currently working were not even born when the FATF released its first-generation recommendations. In this over 30 years long period, AML laws changed bankers' habits and long-standing banking law principles. The number of STRs produced by banks in the last decade clearly

[11] In relation to the failure of voluntary STRs regimes, see pages 29-30 and 65-66 in chapter 2.
[12] The Forty Recommendations of the Financial Action Task Force on Money Laundering 1990 <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf> 10 June 2021.
[13] J Wadsley, 'Money laundering: professionals as policemen' (1994) Conv. 275.
[14] See pages 29-30 and 65-66 at chapter 2.

shows that the STRs regime obtained an essential and well-accepted place in banking law and practice. Europol established in 2017 that the private sector filed more than 6 million SARs across the 28 EU Member States in 9 years from 2006 to 2014, and the banks and credit institutions were the primary source of these reports.[15] It is worth noting that the number of SARs/STRs filed by banks in most countries keeps rising (See charts 1 and 2, which depict the number of reports produced by banks in the last five years in the UK and Switzerland.)

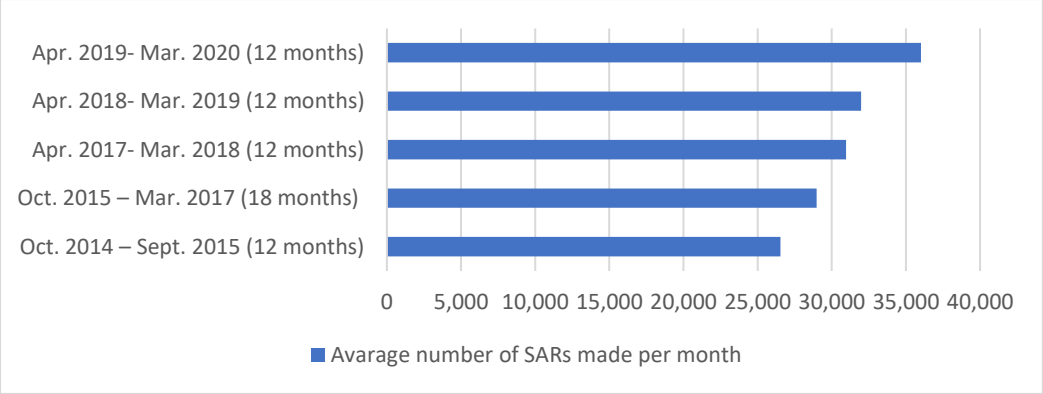


Chart 7: Average number of SARs made by banks per month in the UK[16]

[15] Europol Report, 'From suspicion to action: Converting financial intelligence into greater operational impact' (2017), 14 <https://www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact> 1 June 2021.

[16] This chart was prepared by using information provided in the UKFIU's Annual reports 2020, 2019, 2018, 2017, 2015. See National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2020', (2020), 9; National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2019', (2019), 8; National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2018', (2018), 6; National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2017', (2017), 12; and National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2015', (2015), 9.

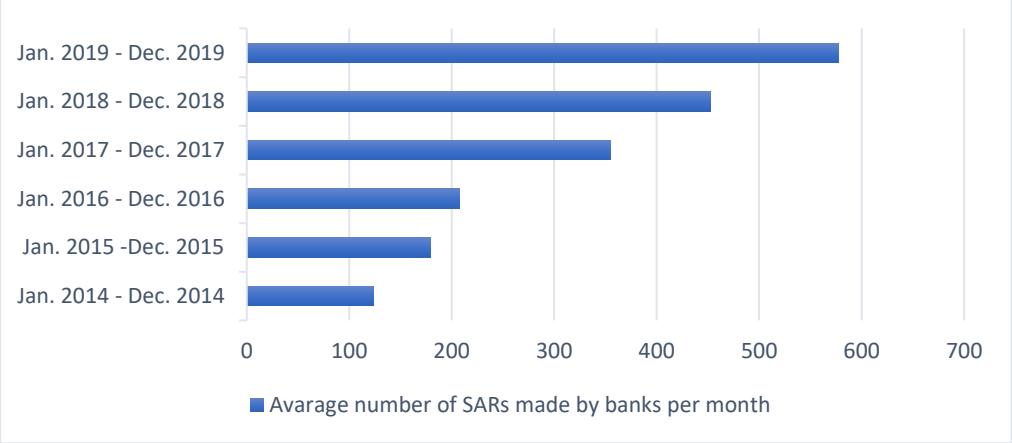


Chart 8: Average number of SARs made by banks per month in Switzerland. [17]

Banks are now making a high number of STRs. Whilst, the effectiveness of the STRs regime is still subject to criticism. One significant problem is the existence of an overwhelming number of low-quality reports. Low-quality reports (eg. reports that contain irrelevant information or that do not contain adequate and accurate information expressing suspicion, reports where the reporting person does not genuinely suspect that funds are the proceeds of crime etc.) cause two problems. First, such reports breach banking clients' information privacy rights. Second, these reports reduce the FIU's capacity to accomplish its duties. Therefore, countries should make the STRs regime reforms to increase the quality of STRs.[18]

STRs produced by banks on the basis of mere suspicion may help the FIUs because even mere suspicion of bankers is likely to be useful to the extent it should be further investigated by a public authority.[19] Low-quality reports, however, have non or few intelligence value for law enforcement authorities in identifying specific targets or money laundering related trends and patterns.[20] For instance, unfounded reports (eg. a report filed with the explanation that 'I am not suspicious of this client but am making this report anyway'[21]) or poorly justified reports (eg. a report justified with merely descriptive information

[17] This chart was prepared by using information provided in the MROS's Annual reports 2019, 2018, 2017, 2016 and 2015. See Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2019', (Avril 2020), 7; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2018', (Avril 2019), 8; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2017', (Avril 2018), 8; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2016', (Avril 2017), 8; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2015', (Avril 2016), 7.

[18] Rt Hon Ben Wallace MP's oral evidence to the Treasury Committee, Economic Crime HC 940 (31 October 2018).

[19] See pages 159-161 in chapter 4.

[20] Law Commission, *Anti-money laundering: the SARs regime* (Law Com No 236, 2018), [6.10].

[21] A low-quality report example given in the NCA's website. NCA's website, 'SAR Quality Issues,: <https://www.ukciu.gov.uk/(b04b1m2pl1jooaqcnqutd3qe)/Information/info.aspx?InfoSection=Quality> 10 June 2021.

such as "Cash transaction £7,000"[22]) would not be of help to the FIUs or other law enforcement authorities. UK Law Commission emphasised that

> while there is an understandable desire among those working in law enforcement to maximise the amount of intelligence and raw data they receive, a large volume of SARs does not guarantee quality of intelligence.[23]

The law enforcement authorities in countries where financial institutions are obliged to make threshold reports naturally receive a high amount of reports (eg. the Netherlands).[24] However, the way in which they are expected to use the threshold reports is different from the way the FIUs are expected to use the STRs. The law enforcement agencies use threshold reports to detect suspicious trends. The FIUs are expected to analyse the STRs to identify specific targets. [25] Hence, they should, ideally, analyse each and all STRs.

Public authorities spend money and use their human resource to analyse unwarranted reports, which in the end, do not provide any helpful information. The unwarranted reports issue is an even more fundamental problem where the FIUs cannot further investigate all the reports they received. It is worth noting that most FIUs cannot examine all the SARs they received. In 2017, Europol established that just 10% of the SARs in the EU were further investigated by the FIUs after collection and this figure was unchanged since 2006**.**[26] By increasing the number of reports received by the FIUs, unwarranted reports shadow reports that may provide essential information. Goldby describes unwarranted reports as 'noise' that distract the attention of law enforcement agencies from the most serious cases.[27] Due to these reports, the FIUs cannot analyse some other reports that may have helped them identify specific targets. The Proceeds of Crime Lawyers Association noted that "valuable resources are deployed trawling through low-grade material, allowing the larger fish and their associated predators to escape detection".[28] The FIUs that cannot investigate all the SARs thoroughly cannot successfully identify money laundering related trends and patterns. Consequently, unwarranted reports cause them to miss the chance to establish more valid and effective policies.

---

[22] A low-quality report example given in the NCA's website. NCA's website, 'SAR Quality Issues,: <https://www.ukciu.gov.uk/(b04b1m2pl1jooaqcnqutd3qe)/Information/info.aspx?InfoSection=Quality> 10 June 2021.

[23] Law Commission, *Anti-money laundering: the SARs regime* (Law Com No 384, 2019), [1.57].

[24] See pages 18-19 in chapter 2.

[25] Interpretive Note to Recommendation 29. FATF (2012-2020), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, 101, <www.fatf-gafi.org/recommendations.html> 10 June 2021;

[26] Europol Report, 'From suspicion to action: Converting financial intelligence into greater operational impact' (2017), 22 <https://www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact> 1 June 2021.

[27] M Goldby, 'Anti-money laundering reporting requirements imposed by English law: measuring effectiveness and gauging the need for reform' [2013] Journal of Business Law 367, 382.

[28] Law Commission (n,23), [1.57].

Moreover, unwarranted reports, which lead low rate of examination, may reduce the deterrent effect of the STRs regime. Indeed, while the fact that the FIUs cannot further investigate almost 90% of the reports is well-known by everyone interested, it might be too optimistic to believe that the STRs regime may successfully deter the offenders.

Furthermore, unwarranted reports constitute an obstacle to the successful application of the Risk-Based Approach. Banks, that are expected to apply a Risk-Based Approach, are expected to identify and assess the money laundering risk to which they are exposed.[29] The FATF's Risk-Based Approach Guidance for the banking sector underlined that "[a]ccess to accurate, timely and objective information about ML.. risks is a prerequisite for an effective RBA"[30]. Case-by-case feedback supplied by the FIUs may help reporters improve their risk analysis.[31] However, the FIUs, which cannot examine approximately 90% of the reports they received, are unable to provide the reporting persons with case by case feedback.[32]

Arguments defended in parts 5.II.A. and 5.II.B. will be supported with examples from the UK and Switzerland.

5.II.C. English AML laws

AML laws that are in breach of information privacy standards lead bankers to make unwarranted reports. The existence of unwarranted reports decrease the success of the country in the fight against economic crime, criminal money and money laundering.

A bank's making of an SAR, authorised or required, often amounts to processing of personal data.[33] Personal data should be processed lawfully.[34] According to article 6(1)c of the UK GDPR, processing shall be lawful if and to the extent that processing is necessary for compliance with a legal obligation to which the controller is subject. Article 6(3) established that the basis for the processing referred to in

[29] FATF, 'Guidance for A Risk-based approach - the banking sector' October 2014, 6 <http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf> 10 June 2021.
[30] Ibid, 8.
[31] Ibid, 10.
[32] Europol (n,26), 45.
[33] A suspicious activity report relating to an individual banking client involves information relating to an identified individual (personal information). Where the customer is a legal person or arrangement, the bank is required to understand the ownership and control structure of the customer. Information relating to the beneficial owner may amount to personal data. Therefore, reports relating to corporate clients may also involve personal information. Disclosure by transmission amounts to processing. Therefore, a bank's making of an SAR often amounts to processing of personal data. See pages 91-95 in chapter 3.
[34] Section 1(b)i of Part 1 of Schedule 2 of DPA 2018 underlined that the lawfulness requirements set out in Article 6 of the UK GDPR are not amongst the listed provisions mentioned in section 5 of Part 1 of Schedule 2 of DPA 2018. Therefore, lawfulness requirements set out in Article 6 would still apply to the banks upon whom POCA 2002 imposed a duty to make SARs under certain conditions. See pages 98-99 in chapter 3.

article 6(1)c shall be laid down by domestic law.[35] "The domestic law shall meet an objective of public interest and be proportionate to the legitimate aim pursued."[36] Public interest referred to in article 6(3) of the UK GDPR includes, amongst others, prevention or prosecution of crime. As part of the proportionality test, domestic law should provide sufficient and adequate guarantees against arbitrariness.[37]

By virtue of Section 5(2) of Part 1 of Schedule 2 of DPA 2018, listed rights of the reported client (eg. right to access, right to information to be provided) are restricted, to the extent that the use of those rights would prevent the controller from making the disclosure.[38] By virtue of Article 23(2) of the UK GDPR, acts that restrict personal data protection rights should contain specific provisions at least, where relevant, as to the safeguards to prevent abuse or unlawful access or transfer.[39]

SARs involve confidential information and banks owe their clients a duty of secrecy.[40] Bankers' duty of secrecy is not absolute but qualified.[41] There are four heads of qualifications, two of which are as follows: [42] Where disclosure is under compulsion by law (eg. "disclosure of suspicion or information about a crime already committed[43]) and where there is a duty to the public to disclose. Similarly, it was recognised in *Attrorney-General v. Guardian Newspapers Ltd* that public interest in the protection of an equitable duty of confidentiality "may be outweighed by some other countervailing public interest which favours disclosure".[44] It is worth noting that the law of confidence should be interpreted in compliance with Article 8 ECHR.[45]

---

[35] Recital 41 of European GDPR prescribes that "Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights."

[36] Section 6(3) of the UK GDPR, similarly see section 6(3) of the EU GDPR.

[37] According to sections 3 and 6 of the Human Rights Act, so far as it is possible to do so, the courts should read and give effect to primary legislation and subordinate legislation in a way which is compatible with the Convention rights. By virtue of section 2, a court determining a question which has arisen in connection with a Convention right must take into account any judgment, decision, declaration or advisory opinion of the ECtHR. See The ECtHR's decisions in *M.N. v San Marino* (2016) 62 E.H.R.R. 19 at [73]. See also *Matheron v France* (57752/00) (Unreported, March 29, 2005) (ECHR), [35]; *Lambert v France* (2000) 30 E.H.R.R. 346, [49]; *Xavier Da Silveira v. France* (43757/05) (Unreported, January 21, 2010) (ECHR), [43] and *Klass and Others* **v**. *Germany (A/28):* (1978) 2 E.H.R.R. 214, [54], [55].

[38] For a list of provisions that are referred to in Section 5(2) of Part 1 of Schedule 2 of DPA 2018, see Section 1 of Part 1 of Schedule 2 of DPA 2018.

[39] Article 23(2) of the UK GDPR.

[40] See pages 101-112 in chapter 3.

[41] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B. 461, at 472-473 (by Bankes LJ)

[42] Ibid.

[43] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B. 461, at 471; Price Waterhouse v BCCI [1992] BCLC 583, 598 (by Millet J.); T Aplin et al., *Gurry on Breach of Confidence* (2nd ed, OUP 2012), [9.53].

[44] *Attrorney-General v. Guardian Newspapers Ltd* (No. 2) [1990] 1 AC 109, 281

[45] Article 8-1 protects, amongst others, one's right to professional confidentiality. *Sommer v Germany* (2018) 67 E.H.R.R. 9, [48]; *M.N. v San Marino* (2016) 62 E.H.R.R. 19, [47]; *Michaud v France* (2014) 59 E.H.R.R 9,

A bank's making of an SAR constitutes an interference with the reported client's right to respect for his private life recognised in Article 8-1 of ECHR.[46] Interference with one's Article 8-1 rights is legitimate where the interference is ""in accordance with the law", pursues one or more of the legitimate aims referred to in paragraph 2 and is, in addition, "necessary in a democratic society" to achieve those aims"[47]. The law must be sufficiently foreseeable in its terms to give individuals an adequate indication as to the circumstances in which their bankers can share their banking data with the law enforcement agencies.[48] One of the legitimate aims referred to in paragraph 2 is "the prevention of disorder or crime". An interference is "necessary in a democratic society" to achieve one or more of the legitimate aims if it is necessary and proportionate to achieve those aims and there exist sufficient and adequate guarantees against arbitrariness.[49] It is worth noting that the ECHR has a special place in the English legal system.[50] First, "[s]o far as it is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with the Convention rights".[51] Second, the Courts should develop and interpret common law in a way that is compatible with the Convention rights.

The extent to which banks are required and permitted to make SARs is determined by the Proceeds of Crime Act 2002. Banks are required and permitted to report their client's 'suspicious' activities. Banks and their staff are not permitted to report whatever they wish to.[52] The Court of Appeal explained the meaning of the word 'suspicion' in section 93A of the Criminal Justice Act 1988 as follows:[53]

> It seems to us that the essential element in the word "suspect" and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice.

Hence, the law is clear, precise and foreseeable. As defended in chapter 2, the notion of suspicions is a matter of common sense and that an informed group such as bankers can scarcely claim that they do not understand it in that the Court of Appeal gives specific guidance in *R v Da Silva*.[54] Banking clients

[118]. The Courts should develop and interpret common law in a way which is compatible with the Convention rights. See pages 126-127 in chapter 3.

[46] Disclosure of banking information by a banker to a public authority without the consent of the data subject may amount to interference for the purposes of Article 8 of ECHR. The ECtHR, in *Sommer v Germany*, established that "making available the applicant's professional bank transactions constituted an interference with his right to respect for professional confidentiality and his private life". (*Sommer v Germany* (2018) 67 E.H.R.R. 9, [48];) See pages 114-116 in chapter 3.

[47] Article 8-2 ECHR; *M.N. v San Marino* (2016) 62 E.H.R.R. 19 at [71]; *Amann v. Switzerland* (2000) 30 E.H.R.R. 843, at [71].

[48] *Fernandez Martinez v Spain* (2015) 60 E.H.R.R. 3, [124].

[49] *M.N. v San Marino* (2016) 62 E.H.R.R. 19, [73]; Matheron v. France, no. 57752/00, § 35, 29 March 2005.

[50] See pages 124-130 in chapter 3.

[51] Section 3 (1) of the Human Rights Act 1998.

[52] *Shah v HSBC Private Bank (UK) Ltd* [2010] 3 All ER 477.

[53] *R v Da Silva* [2006] EWCA Crim 1654, [16].

[54] See also *Michaud v France* (2014) 59 E.H.R.R. 9, [24].

can also understand the extent to which their rights are limited to a reasonable degree, at least with the advice of the experts.[55]

The restriction prescribed by law should pursue a legitimate aim. AML laws relating to the SARs regime pursue a legitimate aim, that is to say detection, prevention and prosecution of crime.[56]

The SARs regime aims to create a system where banks share their money-laundering suspicions with the FIU to increase the law enforcement agencies' capacity to detect criminal money and economic crime.[57] Therefore, requiring and permitting banks to make reports on the basis of suspicion is a necessary measure. However, AML laws relating to the SARs regime did not specify sufficient and adequate safeguards to prevent abuse or unlawful access or transfer. This leads banks' directors, officers, employees and nominated officers to make unwarranted defensive disclosures. The Law Commission reviewed a sample of SARs sent in five consecutive days and found that "reasonable grounds to suspect was present in approximately 53% of the authorised disclosures that [they] analysed and only 32% of required disclosures".[58] Moreover, the Law Commission detected that *Da Silva* test for suspicion was not met in 15% of authorised disclosures and 13% of required disclosures. [59] This means that over 10% of the reports are unwarranted in the sense they do not meet even the low threshold of suspicion and do not reflect the reporter's genuine suspicion.

In the required reports regime, bankers are not permitted to report whatever they wish to.[60] Most importantly, they should be able to show that the information or other matter that they disclosed causes them to know or suspect, or gives them reasonable grounds for knowing or suspecting, that another person is engaged in money laundering. However, no mechanism takes action against those who made unwarranted disclosures. To put it another way, bankers are highly unlikely to stay in a position in which they are obliged to show that the suspicion on which a required SAR they made was founded existed. First, the reported client is highly unlikely to learn that such a report was made. Indeed, tipping off rules and section 5(2) of Part 1 of Schedule 2 of DPA 2018 deprive the client of a chance to learn that its banker made a required report relating to him. Second, the client will not feel anything unusual in his relationship with the bank because the reporting person is not required to freeze the reported client's account.[61] Third, the UKFIU that receives the report is not taking action against unwarranted disclosures. In fact, the UKFIU cannot even examine an important part of the SARs it received. Europol, in 2017, established that between 5-7% of the SARs in the UK were further investigated by the FIU

[55] Dubská and Krejzová v. the Czech Republic (2017) 65 E.H.R.R. 5, [171] and Slivenko v. Latvia (2004) 39 E.H.R.R. 24, [41].
[56] For further details, see pages 154-166 in chapter 4.
[57] See pages 159-161 in chapter 4.
[58] Law Commission (n,20), 47, 95.
[59] Ibid.
[60] See page 63 in chapter 2 in relation to protected disclosure.
[61] See pages 60-63 in chapter 2.

after collection.[62] It is worth noting that these reports further investigated by the UKFIU are consent reports, not required reports. After all, a banker can make an unwarranted required disclosure without worrying about the financial attractiveness and reputation of the bank or legal measures he or the bank may be subject to.

The position is partly different for the authorised reports regime. The UKFIU that receives the reports is not taking action against unwarranted disclosures. However, the legislator created a system with some guarantees against bankers' unwarranted reporting. One who made an authorised disclosure before pursuing a prohibited act must freeze the client's account for a limited time. The client whose account is frozen may face significant financial hardship and loss of reputation. This naturally leads to problems between the reporters and their clients.[63] Where an authorised disclosure is not made in good faith, civil liability arises in respect of the disclosure on the part of the person by or on whose behalf it is made.[64] Hence, an unwarranted disclosure could result in the affected party securing a remedy against the reporter.[65] Moreover, unwarranted authorised reports may adversely affect the bank's reputation.

Above explained difference between the authorised reports regime and the required reports regime is reflected in the numbers. The private sector produces over 14 times more required reports compared to authorised reports. From October 2014 to March 2020, the UKFIU received 162,135 and 2,369,320 authorised and required reports, respectively. This means that 93.5% of the SARs filed were required reports while only 6.5% of the SARs were authorised reports.

[62] Law Commission (n,20), [4.10].
[63] See pages 55-57 in chapter 2.
[64] Sections 338-4A, POCA 2002.
[65] R Fortson QC, 'Money laundering offences under POCA 2002' in W Blair, R Brent and T Grant (eds), *Banks and financial crime – the international law of tainted money* (2nd edn, OUP 2017), 173.

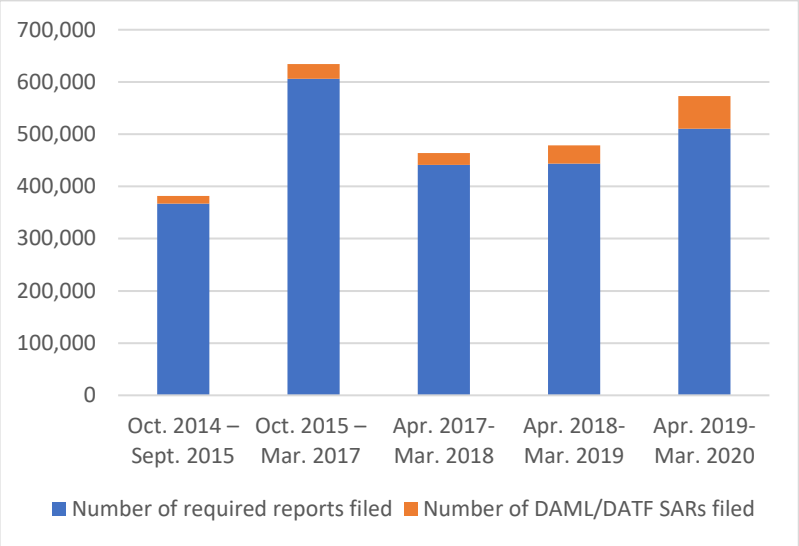


Chart 9: Number of authorised and required SARs filed in the UK from October 2014 to March 2020.[66]

It is understandable that bankers are making a greater number of required reports compared to consent reports. However, if the SARs regime had worked properly, there should not have been such a discrepancy between the number of authorised and required reports filed with the UKFIU. The large disparity in the numbers between consent reports and required reports show that reporters tend to make more and more unwarranted disclosures where the lawmakers failed to take measures against the reporters' abuse of the SARs regime. In their submission to the Law Commission, Dickinson Minto admitted that almost all of the required reports which they have submitted under section 330 of the POCA 2002 relate to matters that they do not genuinely believe are of general use to the NCA nor to the prevention of financial crime.[67]

One who fails to make an authorised disclosure may face more serious punishment.[68] This should incline bankers to make more authorised reports, not required reports. However, there are two reasons that incline bankers to make a higher number of required SARs. First, bankers are inclined to make a greater number of required reports because one is obliged to make an authorised disclosure if he intends to make a prohibited act, while there is no such condition for the required reports specified in sections 330 and 331 of POCA 2002.[69] However, it is worth mentioning that, the ambit of prohibited acts specified

[66] This chart was prepared by using information provided in the UKFIU's Annual reports 2020, 2019, 2018, 2017, 2015. See National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2020', (2020), 9; National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2019', (2019), 8; National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2018', (2018), 6; National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2017', (2017), 12; and National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2015', (2015), 9.

[67] Consultation response of Dickinson Minto, a boutique law firm specialising in corporate matters. Law Commission (n,22), [5.35].

[68] See pages 45-47 in chapter 2.

[69] See pages 60-63 in chapter 2.

in sections 327 to 329 of POCA 2002 is wide.[70] Therefore, a banker who suspects that the funds constitute or represent criminal money is often obliged to make not only a required disclosure but also an authorised disclosure. To put it another way, one who is required to make a required disclosure is highly likely to stay, at some point, in a position where he/she is obliged to make an authorised disclosure (eg. accepting, transferring, or restoring the funds). Therefore, the difference between the number of authorised and required reports is not expected to be excessive.

Second, bankers are inclined to make more required reports because *mens rea* applicable for the offence of money laundering is knowledge or suspicion, while a banker is obliged to make a required disclosure if he knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering.[71] Under sections 330 and 331, the banker must ask themselves two questions. (i) Do I know or do I suspect that the funds constitute or represent proceeds of crime? If the answer is no, the banker should continue with the following question: (ii) Should I know or suspect that the funds constitute or represent proceeds of crime? Authorised disclosures, on the other hand, are deemed to be a declaration that the banker is suspicious. Hence, the intended function of the objective limb in sections 330(2)(b) and 331(2)(b) is to prevent a banker from avoiding liability by declaring that they were not subjectively suspicious. While the objective limb should lead bankers to make a higher number of required disclosures, it should not lead bankers to make unwarranted disclosures due to two reasons. First, the Joint Money Laundering Steering Group Guidance (the JMLG Guidance) shows bankers what they should find suspicious. Second, one does not commit an offence under section 330 of POCA 2002 if he does not know or suspect that another person is engaged in money laundering, and he has not been provided by his employer with such training as is specified by the Secretary of State.[72]

According to Europol's From Suspicion to Action Report published in 2017, 67% of the SARs in the EU were received by the FIUs in two member states: the UK (36%) and Netherlands (31%).[73] Netherland's FIU receives a high number of reports because it receives Unusual transaction reports (UTRs).[74] If the Netherlands was not taken into the calculation, the UKFIU would have been receiving more than half of the STRs made in Europe. It is worth noting that over 90% of these reports are required reports.

The fact that the UKFIU receives a high number of reports is by no means that the SARs regime is successful. The UKFIU can further investigate an overwhelmingly low part of the SARs, because it receives an excessive number of reports, an important part of which are defensive reports. In 2015, the

[70] See pages 42-43 in chapter 2
[71] See Goldby (n,27), 373.
[72] Section 330(7), POCA 2002.
[73] Europol (n,15), 41, chart 2. According to chart 2, the UK FIU and the Netherlands' FIU received 67% of total reports across all Member States (2006 - 2014). Yet, this was mistakenly mentioned as 65% of total reports in pages 5 and 10 of the report.
[74] See pages 18-19 in chapter 2.

Home Office established that financial institutions produce an overwhelming number of defensive reports, "where reports are made more because of concerns regarding a failure to comply with POCA than because of genuine suspicion"[75]. The Law Commission has also made similar observations in its' 2019 SARs regime report.[76] The low quality of reports may be seen by looking at the low percentage of the consent reports that do not receive consent (varied between 11% and 3% from October 2013 to March 2020) (see chart 11 belove). Thus, the UKFIU can further investigate an overwhelmingly low part of the SARs, because it receives an excessive number of reports, an important part of which are defensive reports.

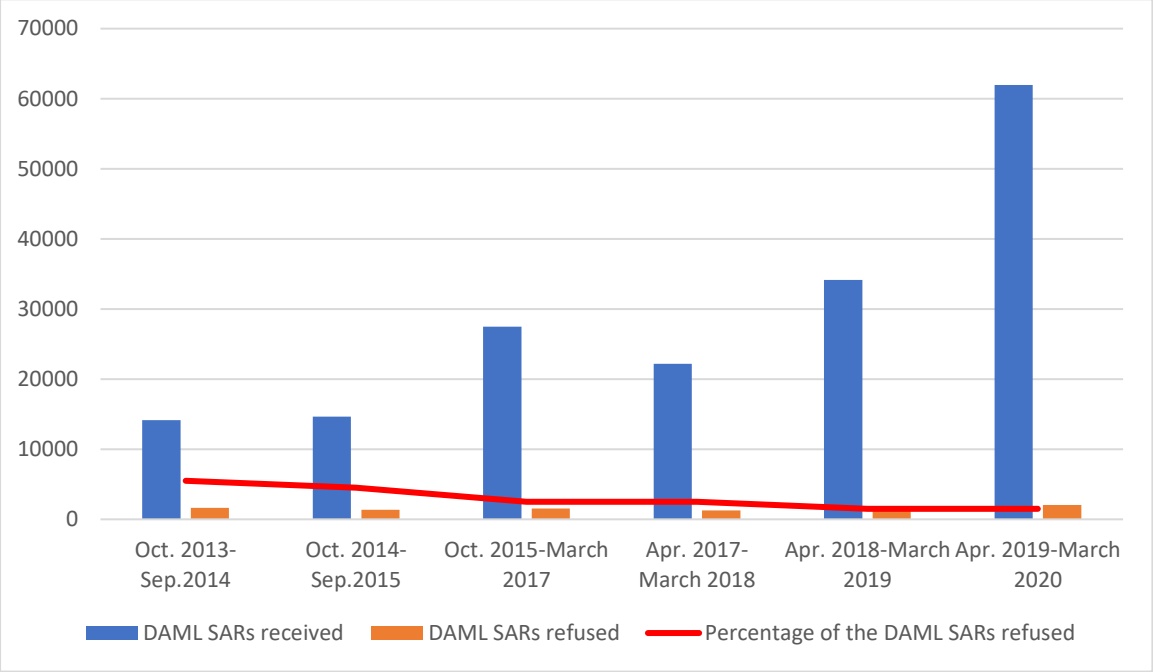


Chart 10: DAML SARs received and refused [77]

The fact that the UKFIU receives a higher number of required reports is by no means that the required reports regime is more successful. In fact, authorised reports regime seems to be more useful because

[75] 'Action Plan for anti-money laundering and counter-terrorist finance – Annex B Findings from the Call for Information on the Suspicious Activity Reports (SARs) Regime' (2016) 39 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/517993/6-2118-Action_Plan_for_Anti-Money_Laundering__print_.pdf> 13 July 2019.

[76] Law Commission (n,20) [1.2]; [1.29] and [4.10]; Law Commission (n,23), [5.12].

[77] This chart was prepared by using information provided in the UKFIU's Annual reports 2020, 2019, 2018, 2017, 2015. See National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2020', (2020), 4; National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2019', (2019), 4; National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2018', (2018), 3; National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2017', (2017), 6; and National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2015', (2015), 6.

the UKFIU uses only authorised SARs as suggested by the FATF.[78] An essential part of the required reports are not analysed further by the UKFIU.

The UKFIU analyses all DAML SARs. However, they do not and are not under a legal duty to analyse all required reports. This is by no means that required reports are not used at all. All reports, authorised or required, are available to a wide range of law enforcement agencies.[79] While the required reports are also of some use, they are not used as the FATF advised. As argued in chapter 4, bankers' suspicion relating to their clients should be taken seriously and further investigated by a law enforcement agency "to identify specific targets (e.g. persons, assets, criminal networks and associations)",[80] and "to identify money laundering and terrorist financing related trends and patterns".[81] Therefore, making reports available to law enforcement agencies is not enough. Hence, the UKFIU cannot benefit from the required reports as they should be due to high number of reports.

The fact that the UKFIU cannot further analyse over 90% of the reports it received hampers the effectiveness of the SARs regime in three points. First, the UKFIU fails to engage with over 90% of the reports which might include useful information. Second, because the UKFIU cannot investigate further all the reports it received, it cannot provide the reporting persons with case-by-case feedback. Therefore, the UKFIU fails to assist reporting persons in ameliorating their risk analysis. Third, because over 90% of the reports cannot be further investigated by the UKFIU, the SARs regime loses its' deterrent effect.

One may defend that the problem of low rate of examination may be resolved by increasing the resources available to the UKFIU. Considering the fact that the UKFIU receives almost one third of the reports made in the EU, it is almost impossible to increase the resources to the extent all the reports are further investigated. Even if resourcing issue is solved and the UKFIU reached at a point it may analyse 14 times more reports per year, the cost effectiveness of the SARs regime will be diminished and the problem between AML laws and privacy will remain unsolved. Therefore, the solution should be increasing the quality of the reports made.

5.II.D. Swiss AML laws

A bank's making of an SAR, permitted or required, amounts to processing of personal data.[82] By virtue of the lawfulness and proportionality principles recognised in the Federal Act on Data Protection 1992

[78] Interpretive note to recommendation 29, *Financial intelligence units*.
[79] Law Commission (n,20), 21-22, 93-95.
[80] Interpretive note to recommendation 29, FATF (n.1), 101-103.
[81] Ibid.
[82] A suspicious activity report relating to an individual or corporate banking client involves information relating to an identified person (personal information). Disclosure by transmission amounts to processing. Therefore, a bank's making of an SAR amounts to processing of personal data. See pages 91-95 in chapter 3.

(FADP 1992), banks can share information relating to their clients with law enforcement agencies the extent to which it is necessary and proportionate to comply with a legal obligation to which they are subject.[83]

Data subject's right to information may be limited where a formal act provides so.[84] Moreover, data controller's duty to provide information on the collection of sensitive personal data and personality profiles ceases to apply if a formal enactment provides so.[85] Formal enactment refers to "1. federal acts, 2. decrees of international organisations that are binding on Switzerland and international treaties containing legal rules that are approved by the Federal Assembly"[86].

SARs involve confidential information and banks owe their clients a duty of secrecy.[87] Bankers' duty of secrecy recognised in Article 47 of the Swiss Banking Act is not absolute. Paragraph 5 of Article 47 stipulates that "[t]he federal and cantonal provisions on the duty to provide evidence or on the duty to provide information to an authority shall be exempted from this provision".[88] Neither does Article 28 of the Code Civil lead an unimpeachable duty of secrecy. According to its' second paragraph, one's relevant rights can lawfully be interfered with if "it is justified by the consent of the person whose rights are infringed or by an overriding private or public interest or by law."

Article 13 of the Federal Constitution of the Swiss Confederation recognises everyone's right to privacy and the right to the protection of personal data. Article 35 of the Federal Constitution recognises vertical and horizontal applicability of fundamental rights. In the Federal Supreme Court's jurisprudence, the right to privacy includes the right to professional confidentiality.[89] By virtue of Article 36 of the Federal Constitution, any law that justifies a breach of the right to privacy or the right to the protection of personal data must be justified in the public interest or for the protection of the fundamental rights of others, must be proportionate and must not touch upon the essence of the rights. In the Federal Supreme Court's jurisprudence, the legal basis mentioned in article 36(1) refers to federal or cantonal law that is clear and precise.[90] Within the scope of the proportionality test, the Federal Supreme Court analyses whether or not there exist sufficient and adequate measures against abuse.[91]

[83] Articles 4(1), 4(2) and 4(4), FADP 1992.
[84] See Articles 8 and 9(1)a, FADP 1992.
[85] Article 14(4)-14(5), FADP 1992.
[86] Article 3, FADP 1992.
[87] See pages 106-112 in chapter 3.
[88] Unofficial translation of Swiss Federal Act on Banks and Savings Banks dated 8 November 1934 (version as at 1 January 2019), translated by KPMG. <https://assets.kpmg/content/dam/kpmg/ch/pdf/ch-banking-act-en.pdf> 1 January 2021.
[89] ATF 103 Ia 293, consid. 4a; ATF 145 IV 144; consid. 2.
[90] ATF 107 Ia 148, consid. 2; ATF 131 II 265, consid. 5.
[91] ATF 124 I 176, consid. 5; ATF 140 I 2, consid. 9.1.

A bank's making of an SAR constitutes an interference with the reported client's right to respect for his private life recognised in Article 8-1 of ECHR.[92] According to article 8-2 of ECHR, interference with one's Article 8-1 rights is legitimate where the interference is ""in accordance with the law", pursues one or more of the legitimate aims referred to in paragraph 2 and is, in addition, "necessary in a democratic society" to achieve those aims"[93]. The law must be sufficiently foreseeable in its terms to give individuals an adequate indication as to the circumstances in which their banker can share their banking data with the law enforcement agencies.[94] One of the legitimate aims referred to in paragraph 2 is "the prevention of disorder or crime". An interference is "necessary in a democratic society" to achieve one or more of the legitimate aims if it is necessary and proportionate to achieve those aims and there exist sufficient and adequate guarantees against arbitrariness.[95] It is worth noting that section I of the ECHR is of supra-legislative value. Therefore, all federal and cantonal laws should comply with the ECHR.[96]

Article 305ter paragraph 2 of the Swiss Criminal Code and Article 11 of the Anti-Money Laundering Act 1997 (AMLA 1997) permit banks to make permitted and required SARs, respectively. Article 9 of the Anti-Money Laundering Act 1997 impose upon banks a duty to make required SARs. To show the relationship between information privacy standards and the success of the SARs regime, this chapter focuses on the required SARs regime.

The extent to which banks are obliged and permitted to make required disclosure is determined in AMLA 1997. Article 9 of AMLA 1997 impose upon banks duty to make a required SAR where they have a well-founded suspicion as to the legal origin of the asset. The Federal Council, in its' 1996 report that introduced Anti Money Laundering Bill, defended that suspicion is deemed well-founded "where there are concrete signs or several indicia that suggest the origin of the assets is unlawful".[97] However, the courts and the MROS interpreted 'well-founded suspicion' more extensively. Accordingly, there is well-founded suspicion where there is mere doubt as to the legal origin of asset.[98] The Federal Supreme

[92] Disclosure of banking information by a banker to a public authority without the consent of the data subject may amount to interference for the purposes of Article 8 of ECHR. The ECtHR, in *Sommer v Germany*, established that "making available the applicant's professional bank transactions constituted an interference with his right to respect for professional confidentiality and his private life". (*Sommer v Germany* (2018) 67 E.H.R.R. 9, [48];) See pages 114-116 in chapter 3.
[93] *M.N. v San Marino* (2016) 62 E.H.R.R. 19 at [71]; *Amann v. Switzerland* (2000) 30 E.H.R.R. 843, at [71].
[94] Fernandez Martinez v Spain (2015) 60 E.H.R.R. 3, [125]
[95] *M.N. v San Marino* (2016) 62 E.H.R.R. 19 at [73]; Matheron v. France, no. 57752/00, § 35, 29 March 2005.
[96] See pages 118-124 in chapter 3.
[97] « Message relatif à la loi fédérale concernant la lutte contre le blanchissage d'argent dans le secteur financier, 96.055 » FF 1996 III 1057, 1086.
[98] TF, 20 decembre 2013, BB.2013.115; *ATF* 128 IV 145 ss, *JdT* 2004 IV 32, *SJ* 2002 I 565; *ATF* 142 IV 333; Office fédéral de la police (n.408), 86; FATF (2016), Anti-money laundering and counter-terrorist financing measures - Switzerland, Fourth Round Mutual Evaluation Report, FATF, Paris, France, 195 <www.fatf-gafi.org/publications/mutualevaluations/documents/mer-switzerland-2016.html> 10 June 2021.

Court takes into account banking institutions' customer due diligence duties in deciding whether there is a doubt as to the legal origin of assets.[99]

Article 11 of AMLA 1997 reads as follows:

> Any person who in good faith files a report under Article 9 of this Act or who freezes assets in accordance with Article 10 may not be prosecuted for a breach of official, profession or trade secrecy or be held liable for breach of contract.

Hence, the reporter who is protected by Article 11 is one who had a pertinent reason to think that there is doubt as to the legal origin of the assets. Hence, banks and their staff are not permitted to report whatever they wish to.

Relevant articles of AMLA 1997 pursue a legitimate aim, that is to say detection, prevention and prosecution of crime. To pursue this aim, the law-maker aimed to create a system where banks share their money-laundering suspicions with competent public authorities. As shown in previous chapter 4, the establishment of such a system is necessary for fighting against economic crime, criminal money and money laundering. Therefore, requiring and permitting banks to report their suspicion is a necessary measure. However, there are no sufficient and adequate safeguards to prevent abuse in the current required SARs regime.

In 1997, the required reports regime was established with some guarantees against bankers' unwarranted reporting. Until 1 January 2016, a financial intermediary who filed a required report was immediately under a duty to freeze the relevant client's account for five working days unless the MROS informs the reporting person that such measure is unnecessary.[100] The client whose account is frozen may face significant financial hardship and loss of reputation, and the reporter who made a report without a pertinent reason that justifies their filing the report is responsible for damages of the client.[101] Moreover, unwarranted reports may adversely affect the bank's reputation. Hence, the required reports system was established with some guarantees against bankers' unwarranted reporting.

The above-explained system was changed in 2015, and the new rules entered into force on 1 January 2016. Currently, during the analysis conducted by the MROS of a required report, the financial intermediary shall execute customer orders relating to the assets reported under Article 9 -1(a) of AMLA 1997.[102] While this reform has made making an SAR easier and safer, the law-maker did not take any further measures against bankers' abuse of the reporting system. Therefore, the Swiss required SARs system resembles the English required SARs system since 2016. First, the client cannot learn that an

[99] ATF 136 IV 188, 3 November 2010. FATF (2016), Anti-money laundering and counter-terrorist financing measures - Switzerland, Fourth Round Mutual Evaluation Report, FATF, Paris, France, 158 <www.fatf-gafi.org/publications/mutualevaluations/documents/mer-switzerland-2016.html> 10 June 2021.
[100] Article 10, AMLA 1997.
[101] C Lombardini, *Banques et blanchiment d'argent* (3rd éd, Schulthess 2016), 162 ; See page 80 in chapter 2.
[102] Article 9a, AMLA 1997.

SAR relating to him/her was made.[103] Second, the client will not feel anything unusual in his relationship with its bank because the reporting banker is not required to freeze the client's account. Third, the MROS, the authority which receives the SARs, is not taking action against unwarranted disclosures.

The above-explained legal revision in 2016 significantly affected the number of required reports made by private entities. The number of required reports the MROS received in 1 year increased by 350% from 2016 to 2019.

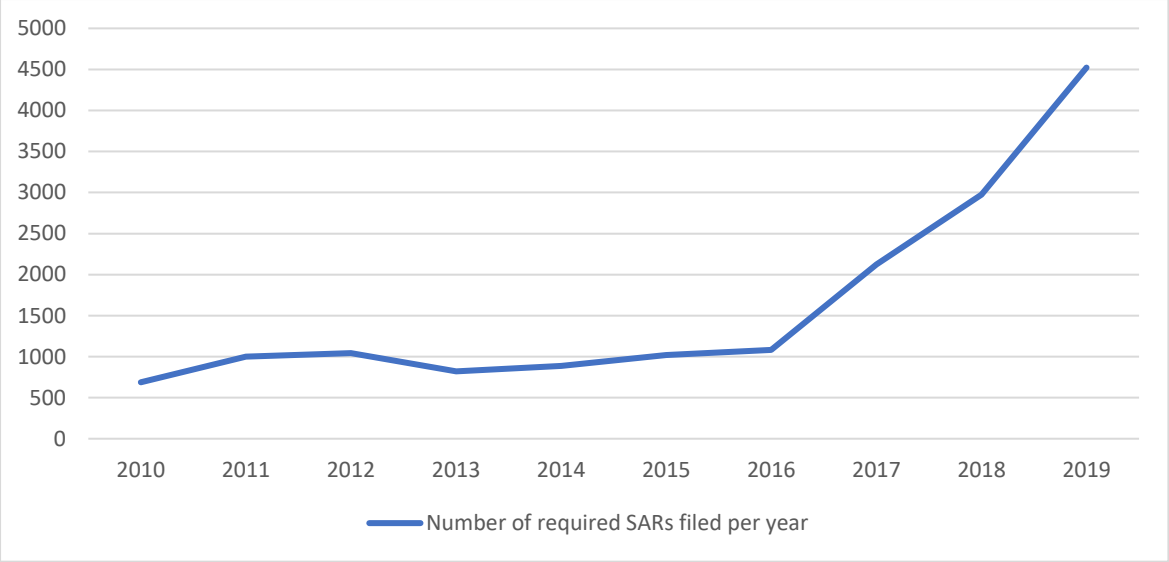


Chart 11. Number of required SARs filed per year[104]

In its 2011 annual report, the MROS put it that: [105]

> The efficiency and effectiveness of money laundering legislation should not only be measured against the number of reports or statistics, but – more relevantly – by comparing the proportion of forwarded reports.

The MROS's statistics show that while it forwarded to the prosecution authorities 74.3% of the SARs it examined in 2016, this number reduced to %49.6 in 2019. This may indicate a decline in the quality

[103] See page 80 in chapter 2.
[104] See Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2019', (Avril 2020), 7; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2018', (Avril 2019), 8; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2017', (Avril 2018), 8; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2016', (Avril 2017), 8; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2010', (Avril 2011), 9; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2005', (Avril 2016), 9.
[105] Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2011', (Avril 2012), 15.

of the reports the MROS received. However, the MROS or other federal authorities have not yet conducted any published research to examine the quality of the SARs MROS received.

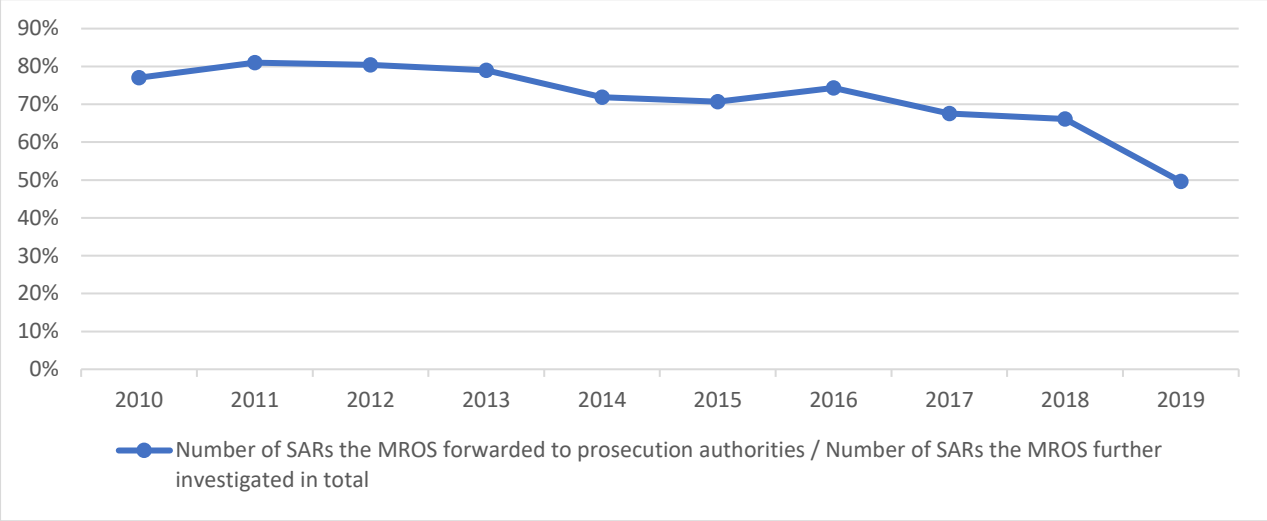


Chart 12: Percentage of the SARs forwarded to prosecution authorities[106]

As explained in previous chapter 4, the FIUs should take transactions that bankers found suspicious seriously. Until 2015, the MROS was able to analyse all the SARs it received. In 2016, this also changed. While the MROS is still successful compared to its homologues, it is worth noting that the percentage of the SARs the MROS investigated further reduced by 48% in 5 years.

[106] See Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2019', (Avril 2020), 7; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2018', (Avril 2019), 8; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2017', (Avril 2018), 8; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2016', (Avril 2017), 8; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2010', (Avril 2011), 9; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2005', (Avril 2016), 9.

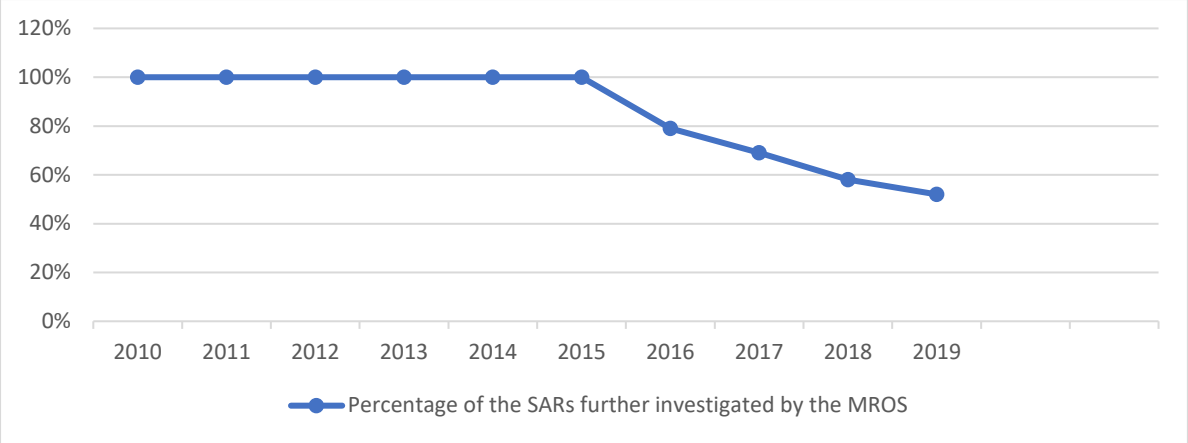


Chart 13: Percentage of the SARs further investigated by the MROS[107]

All the statistics indicate that the MROS may be receiving more and more low-quality reports. However, the MROS has not yet published a report focusing on this issue. Dr Tom Fisher, Privacy International's FinTech lead, established, in 2017 Privacy International Policy meeting, that the UK is not the only country that is affected by the unwarranted STRs problem. However, it seems that the UK is the only country that is aware of the fact that it is affected by this problem.[108]

5.II.E The FATF's position

The FATF's recommendation 2 reads as follows:

> Countries should have national AML/CFT/CPF policies, informed by the risks identified, which should be regularly reviewed, and should designate an authority or have a coordination or other mechanism that is responsible for such policies.
>
> Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policymaking and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate and exchange information domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of

[107] See Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2019', (Avril 2020), 7; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2018', (Avril 2019), 8; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2017', (Avril 2018), 8; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2016', (Avril 2017), 8; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2010', (Avril 2011), 9; Office fédéral de la police, 'Bureau de Communication en Matière de Blanchiment d'Argent (MROS) Rapport Annuel 2005', (Avril 2016), 9.

[108] T Fisher, PI Policy Meeting, speaker.

> proliferation of weapons of mass destruction. This should include cooperation and coordination between relevant authorities to ensure the compatibility of AML/CFT/CPF requirements with Data Protection and Privacy rules and other similar provisions (e.g. data security/localisation).

Recommendation 2 is on 'national cooperation and coordination'. The FATF advised the establishment of mechanisms that would facilitate such cooperation and referred to data protection and privacy rules within this context. However, Recommendation 2 is still an important step because it shows that the FATF, the international organisation that is establishing international AML standards, does not associate information privacy laws with economic crime. It advises relevant authorities to ensure AML rules' compatibility with data protection and privacy rules.

This thesis showed that the STRs regime related AML laws that are in breach of information privacy rules hamper the effectiveness of the STRs regime. The FATF, in its' recommendation 2, advises competent authorities to make an effort to ensure the compatibility of AML requirements with Data Protection and Privacy rules and other similar provisions. Moreover, in its' recommendations 20 and 21, the FATF advises countries to establish a system where financial institutions report their client's suspicious transactions. Therefore, the FATF should attach great importance to the STRs regime related AML laws' compatibility with information privacy rules. The FATF officials, however, seem to be reluctant to deal with this issue. Neither in Interpretive Notes nor in the relevant parts of the mutual evaluation reports did the FATF officials explain or investigate the relation between information privacy laws and the STRs.[109] It is worth mentioning that the FATF's last Mutual Evaluation Report relating to the implementation of AML/CTF standards in the UK, which was produced after an on-site visit which took place after the integration of the second sentence of paragraph 2 of the recommendation 2, did not question whether and to what extent the SARs regime in the UK is compatible with privacy and data protection laws.[110]

5.III. Recommendations

This thesis submitted that an effective Suspicious Transaction Reports STRs regime may be established by protecting banking clients' information privacy rights. As Benjamin Franklin cleverly submitted more than 200 years ago, we need to preserve, not give up, freedom to gain and deserve security.[111]

---

[109] Interpretive Note to Recommendation 2; FATF (2018), Anti-money laundering and counter-terrorist financing measures – United Kingdom, Fourth Round Mutual Evaluation Report, FATF, Paris, France <http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-kingdom2018.html> 10 June 2021; See also FATF (2020), Anti-money laundering and counter-terrorist financing measures - Switzerland, Enhanced Follow-up Report & 2nd Technical Compliance Re-Rating, FATF, Paris, 11 <http://www.fatf-gafi.org/publications/mutualevaluations/documents/fur-switzerland-2020.html>

[110] FATF (n,109), 4.

[111] A letter believed to have been written by Benjamin Franklin in 1755 on behalf of the Pennsylvania Assembly to the colonial governor.

This thesis has shown that the STRs regime is in failure, partly because AML laws requiring and permitting banks to make STRs are incompatible with the legal instruments that protect banking clients' right to the protection of personal data. Therefore, this thesis submits that the STRs regime needs to be re-designed considering relevant information privacy laws.

The UK's FIU seems to receive an excessive number of unwarranted reports. English legislator should make STRs regime reforms to increase the quality, not quantity of SARs. A comparison of the authorised and required SARs regimes show that making bankers responsible for producing unwarranted reports may be an effective way to eliminate unwarranted reports. Therefore, relevant authorities should take sufficient and adequate safeguards against unwarranted reports. For instance, banks or banking staff that repeatedly produce clearly unwarranted reports may be subject to sanction. This may be done by the National Crime Agency that is the UK's Financial Intelligence Unit, the Financial Conduct Authority that is the primary financial regulator so far as regulation in relation to financial crime is concerned, or the Information Commissioner's Office. They may prefer a name and shame method by declaring to the public a list of banking institutions whose nominated officers often make manifestly unwarranted disclosures. The risk of losing attractiveness and reputation may lead banks to take necessary measures against unwarranted disclosures.

Switzerland's FIU is amongst the FIUs receiving the lowest number of reports from financial institutions. However, this is by no means Swiss FIU does not receive low-quality disclosures. Indeed, an FIU may receive few reports, but an important part of these reports can be unwarranted. MROS has not published any data in relation to the proportion of unwarranted reports. However, there are some indicators which show that MROS may also be facing an unnecessary reports issue. The MROS that is no more able to further investigate all the reports it received should also provide further information relating to the quality of the SARs it received.

The FATF should take further action to underline the importance of interpreting its' other recommendations in compliance with data protection and privacy laws. First, the FATF should further clarify what data protection and privacy principles it is referring to. This may be done by providing further explanation or referring to an international data protection rights instrument in the interpretive note to recommendation 2. Second, the FATF should stress out that recommendation 21 should be interpreted and given effect in compliance with data protection and privacy rules. This may be done by drafting an interpretive note to recommendation 21. Examining STRs related AML laws' compatibility with information privacy laws in mutual evaluation reports may also lead countries to establish STRs regime where reporters make high-quality reports.

BIBLIOGRAPHY

Statutes

The UK

Crime and Courts Act 2013

Criminal Justice Act 1988

Criminal Justice Act 1998

Criminal Law Act 1977

Data Protection Act 1984

Data Protection Act 1998

Data Protection Act 2018

Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019/419

Drug Trafficking Act 1994

Drug Trafficking Offences Act 1986

Financial Services and Markets Act 2000

Human Rights Act 1998

Investigatory Powers Act 2016

Misuse of Drugs Act 1971

Money laundering Regulations 2017 (Regulations 2017)

POCA 2002 (References to Financial Investigators) (Amendment) Order 2009

POCA 2002 (References to Financial Investigators) (England and Wales) Order 2015

Police Act 1997

Prevention of Terrorism (Temporary Provisions) Act 1989

Proceeds of Crime Act 2002

Regulation of Investigatory Powers Act 2000

Serious Organised Crime and Police Act 2005

Terrorism Act 2000

UK General Data Protection Regulation

Switzerland

Anti-Money Laundering Act 1997

Civil Code

Code of Obligations

Criminal Code 1937

Federal Act of 14 December 1993 on Direct Federal Taxation

Federal Act of 14 December 1994 on the Harmonisation of Direct Federal Taxation at Cantonal and Communal Levels.

Federal Act on Administrative Criminal Law 1974

Federal Act on Banks and Saving Banks 1934

Federal Act on Data Protection 1992

Federal Act on Narcotics and Psychotropic Substances

Federal Act on Narcotics and Psychotropic Substances.

FINMA Anti-money laundering ordinance'

Ordinance on the Federal Act on Data Protection 1993 (Ordinance 1993)

Revised-Data Protection Act 2020

Swiss Federal Constitution

France

Monetary and Financial Code.

The Netherlands

Money Laundering and Terrorist Financing (Prevention) Act (Wwft).

USA

The Gramm-Leach-Bliley Act 1999, Pub L No 106-102, 106th Congress, 1st Sess (12 November 1999) 113 Stat 1338 -1481 (1999).

International Instruments

FATF (2012-2020), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, 19, <www.fatf-gafi.org/recommendations.html> 10 June 2021.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

The Charter of Fundamental Rights of the European Union

The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108)

The Forty Recommendations of the Financial Action Task Force on Money Laundering 1990 <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf> 10 June 2021.

The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988, (Vienna Convention)

The United Nations Convention against Transnational Organized Crime, 2000 (Palermo Convention),

United Nations Convention Against Corruption, 31 October 2003

Cases

UK

A-G v Guardian Newspapers (No. 2) (1990) 1 AC 109

Amalgamated Metal Trading Ltd v City of London Police Financial Investigation Unit [2003] 1 WLR 2711

AP, U Limited v CPS, RCPO [2007] EWCA Crim 3128

Australian Bank Limited (1920) AC 683

Barclays Bank Plc v Taylor [1989] 1 WLR 1066

Beer v Ward (1821) Jac 77, 37 ER 779

Brutus v Cozens (1972) 56 Cr. App. R. 799

Coco v A N Clark (Engineers) Limited (1969) PRC 41

Commissioners of Taxation v English, Scottish and Australian Ltd. [1920] AC 83

Davies v Clough (1837) 8 Sim 262, 59 ER 105

Foster v Bank of London (1862) 176 ER 96

Franklin v Giddings [1978] 1 Qd R 72)

Governor and Company of the Bank of Scotland v A Ltd [2001] 1 WLR 751

Hardy v Veasey [1868] LR 3 Ex. 107

Hellewell v Chief Constable of Derbyshire [1995] 1 WLR 804

Johnson v Marriott (1833) 2 C & M 183, 149 ER 725

K Ltd v National Westminster Bank [2006] EWCA Civ 1039

Ladbroke and Co v Todd (1914) 30 TLR 433

Lennard v Asiatic Petroleum [1915] AC 705

Lewis v Smith (1849) 41 ER 1326

Lipkin Gorman v. Kapnale Ltd [1989] 1 WLR 1340

Llyods Bank v The Chartered Bank of India, Australia and China [1929] 1 KB 40

McKennit v Ash [2008] QB 73

Morison v London County and Westminster Bank, Limited [1914] 3 K. B. 366

Nichotherm Electrical Co Ltd v Percy [1957] RPC 207

Pollard v Photographic Co (1889) 40 Ch D 345

Price Waterhouse v BCCI [1992] BCLC 583

R v Barnham [2005] EWCA Crim 1049

R v Benjafield [2001] 3 WLR 74

R v Bowbotham [2006] EWCA Crim 747

R v Da Silva [2006] EWCA Crim 1654

R v Foggom [2003] EWCA Crim 270

R v Gabriel [2006] EWCA Crim 229

R v Granger [2007] EWCA Crim 139

R v Griffiths [2006] EWCA Crim 2155

R v Homer [2006] EWCA Crim 1559

R v IK [2007] EWCA Crim 491

R v Montila [2004] 1 W.L.R. 3141

R v Pace [2014] EWCA Crim 186

R v Saik [2007] 1 AC 18

R v Sekhon [2002] EWCA Crim 2954

R v Smith [2001] UKHL 68

R v Swan [2011] EWCA Crim 2275

R v Thomas [2014] EWCA Crim 1958

R v W and C [2008] EWCA Crim 2

R. v Lane (Sally) [2018] UKSC 36

Saltman Engineering Co. Ltd v. Campbell Engineering Co. Ltd (1948) 65 R.P.C. 203

Shah v HSBC [2012] EWHC 1283

Shah v HSBC Private Bank (UK) Ltd [2010] 3 All ER 477

Squirrell Ltd v National Westminster Bank plc [2005] 2 All ER 784

Tassell v Cooper (1850) 137 ER 990

Taylor v Blacklow (1836) 3 Bing (NC) 235, 32 ER 401

Tesco Supermarkets Ltd v Nattrass [1972] AC 153

Tournier v. National Provincial and Union Bank of England (1924)1 KB 461

Weld-Blundell v. *Stephens* [1920] A. C. 956

Switzerland

ATF 103 Ia 293

ATF 106 Ia 180

ATF 106 Ia 406

ATF 107 Ia 148

ATF 111 Ia 239

ATF 111 V 203

ATF 112 II 1

ATF 112 II 13

ATF 116 IV 269

ATF 117 Ib 367

ATF 117 Ib 369

ATF 118 Ib 281

ATF 119 V 171

ATF 120 IV 323

ATF 120 IV 365

ATF 122 IV 211

ATF 123 IV 70

ATF 124 I 176

ATF 124 I 6

ATF 124 IV 274

ATF 125 II 417

ATF 126 II 324

ATF 126 IV 255

ATF 127 IV 20

ATF 128 II 211

ATF 128 IV 145

ATF 129 IV 238

ATF 129 IV 322

ATF 131 II 265

ATF 131 III 217

ATF 134 IV 185

ATF 136 I 297

ATF 136 IV 179

ATF 136 IV 188

ATF 138 IV 1

ATF 139 I 16

ATF 140 I 2

ATF 142 IV 333

ATF 145 IV 144

ATF 64 (1938) II 162

ATF 82 II 555

ATF 94 I 669

ATF 99 Ib 39

BGer 6S. 595/1999 of 24 Janvier 2000

Cour de cassation, Genève, 22 novembre 1996, *SJ* 1997 186 ss.

TF 1B 421/2011, 22 Décembre 2011

TF 6B 313/2008, 25 Juin 2008; ATF 120 IV 365, 19 Décembre 1994

TF, 11 mai 2009, 6B_1035/2008

TF, 12 aout 2008, 6B_482/2007

TF, 14 aout 2002, 6S.702/2000

TF, 14 novembre 2007, 6B_369/2007

TF, 14 novembre 2007, 6B_369/2007

TF, 16 mars 2012, 6B_682/2011

TF, 17 aout 2015, 6B_408/2015

TF, 18 juillet 2013, 6B_627/2012

TF, 19 septembre 2007, 1S.32/2006

TF, 2 décembre 2013, BB.2013.146

TF, 20 avril 2009, 6B_835/2008, TF, 18 juillet 2013, 6B_627/2012

TF, 20 décembre 2013, BB.2013.115

TF, 20 mai 2009, 6B_1021/2008

TF, 21 octobre 2010, 6B_900/2009

TF, 22 avril 2005, 1S.13/2005

TF, 22 septembre 2006, 6S.302/2006

TF, 23 juin 2015, 6B_990/2014

TF, 23 mars 2001, 6S.778/2000

TF, 24 mars 2013, 1B_711/2012

TF, 25 février 2015, 6B_508/2014

TF, 25 juin 2007, 6P.49/2007

TF, 26 Avril 2011, 6B_91/2011

TF, 26 mai 2003, 6S.709/2000

TF, 27 septembre 2013, 1B_213/2013

TF, 28 avril 2003, 1P.120/2003

TF, 28 décembre 2006, 6S.426/2006

TF, 29 mars 2006, 4C.33/2006

TF, 4 avril 2003, 6S.226/2002

TF, 5 mai 2003, 6S.35/2003

TF, 7 février 2005, 6P.142/2004

TF, 8 décembre 2011, 6B_729/2010

TF, 8 février 2006, 6S.265/2005

TF, 8 février 2006, 6P.117/2005

TF, 8 juillet 2014, 6B_864/2013

TF, 8 septembre 2003, 6S.22/2003

TF,12 mai 2006, 1P.81/2006

TPF, 10 octobre 2008, SK.2007.24

TPF, 16 mars 2015, BB.2014.157

TPF, 2 décembre 2013, BB.2013.146

TPF, 20 décembre 2013, BB.2013.115

USA

Capone v. United States, 51 F.2d 609 (7th Cir. 1931)

Graney development Corp v Taksen 92 Misc 2d 764 (NY Sup Ct 1978)

US v $4,255,625.39 (1982) 551 F sup.314

France

CA Paris, 6 févr. 1975, O. 1975, p. 318,

ECHR

Amann v. Switzerland (2000) 30 E.H.R.R. 843

André and Another v. France (24 July 2008)18603/03

Armoniene v Lithuania (2009) 48 E.H.R.R. 53

Brito Ferrinho Bexiga Villa-Nova v Portugal (69436/10) (Unreported, December 1, 2015) (ECHR)

Cremieux v France (1993) 16 E.H.R.R. 357

Dubská and Krejzová v. the Czech Republic (2017) 65 E.H.R.R. 5

Dudgeon v. the United Kingdom (1983) 5 E.H.R.R. 573

Evans v. the United Kingdom (2008) 46 E.H.R.R. 34

Fernandez Martinez v Spain (2015) 60 E.H.R.R. 3

I v Finland (2009) 48 E.H.R.R. 31

Johansen v. Norway (1997) 23 E.H.R.R. 33

Klass and Others ***v****. Germany (A/28):* (1978) 2 E.H.R.R. 214

Kroon v. the Netherlands (1995) 19 E.H.R.R. 263

Kruslin v. France [1990] 4 WLUK 184

Lambert v France (2000) 30 E.H.R.R. 346

Leander v Sweden (1987) 9 E.H.R.R. 433

Libert v France, App no 588/13, Fifth Chamber of the European Court of Human Rights, 22 February 2018

M.N. v San Marino (2016) 62 E.H.R.R. 19

Matheron v France (57752/00) (Unreported, March 29, 2005) (ECHR)

Michaud v France (2014) 59 E.H.R.R 9

Niemietz v Germany (1993) 16 E.H.R.R. 97

Perry v the United Kingdom (2004) 39 E.H.R.R. 3

Rotaru v Romania [2000] 5 WLUK 77

Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland (2018) 66 E.H.R.R. 8

Shimovolos v. Russia, (2014) 58 E.H.R.R. 26

Silver v. the United Kingdom, (1981) 3 E.H.R.R. 475

Slivenko v. Latvia (2004) 39 E.H.R.R. 24

Sommer v Germany (2018) 67 E.H.R.R. 9

Uzun v Germany (2011) 53 E.H.R.R. 24

Wieser and Bicos Beteiligungen GmbH v Austria (2008) 46 E.H.R.R. 54

X and Y v Netherlands (1985) 8 EHRR 235

Xavier Da Silveira v. France (43757/05) (Unreported, January 21, 2010) (ECHR)

Z v Finland (1998) 25 E.H.R.R. 371

Report, Guidance, Bill

The UK

Action Plan for anti-money laundering and counter-terrorist finance – Annex B Findings from the Call for Information on the Suspicious Activity Reports (SARs) Regime' (2016) 39 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/517993/6-2118-Action_Plan_for_Anti-Money_Laundering__print_.pdf> 13 July 2019.

Annex B - The substantive UK law on money laundering in "Money Laundering Legislation: Guidance for Solicitors" (The Law Society, 14 August 2002).

CPS, 'Proceeds Of Crime Act 2002 Part 7 - Money Laundering Offences', Legal Guidance,

Financial Conduct Authority Guidance (FCA Guidance)

Financial Conduct Authority Handbook (FCA Handbook)

Hansard (House of Lords) vol. 637, cols. 156, 157 6 March 2018.

HM Treasury and Home Office (UK), 'UK National Risk Assessment of Money Laundering and Terrorist Financing', October 2015.

HM Treasury, 'Money Laundering Regulations 2007: Summary of Responses to consultation on draft Regulations' July 2007.

JMLSG, Prevention of Money Laundering, 2009.

Joint Money Laundering Steering Group Guidance (JMLSG Guidance)

Kerry Report, 1992, vol 1.

Law Commission, *Anti-money laundering: the SARs regime* (Law Com No 384, 2019)

Law Commission, *Anti-money laundering: the SARs regime* (Law Com No 236, 2018)

National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2020', 2020.

National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2019', 2019;

National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2018', 2018;

National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2017', 2017;

National Crime Agency, 'UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2015', 2015.

the Treasury Committee, Economic Crime HC 940 (31 October 2018).

Switzerland

« Initiative populaire fédérale « Le droit suisse au lieu de juges étrangers (initiative pour l'autodétermination) » ». <https://www.bk.admin.ch/ch/f/pore/vi/vis460t.html> 10 June 2021.

« Initiative populaire fédérale «Oui à la protection de la sphère privée». Retrait » FF 2018 212

« Message relatif à la loi fédérale concernant la lutte contre le blanchissage d'argent dans le secteur financier, 96.055 » FF 1996 III 1057

«Arrêté fédéral relatif à l'initiative populaire «Oui à la protection de la sphère privée» (Projet) », FF 2015 6467.

«Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales», 10 Aout 2017, <https://www.admin.ch/ch/f/gg/pc/documents/2826/Revision-totale-de-la-loi-sur-la-protection-des-donnees_Rapport-resultats_fr.pdf> 10 June 2021

«Message concernant la modification du code pénal suisse et du code pénal militaire» FF 1993 III 269.

13.4258 - Interpellation, ‘Pourquoi y-a-t-il tant de coupures de 1000 francs en circulation depuis 2008?’ <https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20134258> 1 June 2021 ; and

16.3114 – Interpellation, ‘Engouement pour les billets de 1000 francs. La réputation de la Suisse est-elle en danger?’ <https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163114>

Arrêté du Conseil fédéral constatant le résultat de la votation populaire du 25 novembre 2018 – Article 2(2). <https://www.bk.admin.ch/ch/f/pore/vi/vis460.html> 10 June 2021.

FF 2010 2067 « La relation entre droit international et droit interne » in Rapport du Conseil fédéral, 5 March 2010, <https://www.admin.ch/opc/fr/federal-gazette/2010/index_13.html> 10 June 2021.

Office fédéral de la police, ‘Bureau de Communication en Matière de Blanchiment d‘Argent (MROS) Rapport Annuel 2007’, (Avril 2007)

Office fédéral de la police, ‘Bureau de Communication en Matière de Blanchiment d‘Argent (MROS) Rapport Annuel 2019’, (Avril 2020);

Office fédéral de la police, ‘Bureau de Communication en Matière de Blanchiment d‘Argent (MROS) Rapport Annuel 2018’, (Avril 2019);

Office fédéral de la police, ‘Bureau de Communication en Matière de Blanchiment d‘Argent (MROS) Rapport Annuel 2017’, (Avril 2018);

Office fédéral de la police, ‘Bureau de Communication en Matière de Blanchiment d‘Argent (MROS) Rapport Annuel 2016’, (Avril 2017);

Office fédéral de la police, ‘Bureau de Communication en Matière de Blanchiment d‘Argent (MROS) Rapport Annuel 2015’, (Avril 2016).

Office fédéral de la police, «Bureau de Communication en Matière de Blanchiment d‘Argent (MROS) Rapport Annuel 2012» July 2012

Office fédéral de la police, «Bureau de Communication en Matière de Blanchiment d‘Argent (MROS) Rapport Annuel 1998/1999», July 1999

Office fédéral de la police, «Bureau de Communication en Matière de Blanchiment d‘Argent (MROS) Rapport Annuel 1999/2000» June 2020

Office fédéral de la police, «Bureau de Communication en Matière de Blanchiment d‘Argent (MROS) Rapport Annuel 2000» July 2001

Office fédéral de la police, «Bureau de Communication en Matière de Blanchiment d‘Argent (MROS) Rapport Annuel 2001» May 2002

Projet de loi, FF 2017 6803

Rapport du groupe interdépartemental de coordination sur la lutte contre le blanchiment d’argent et le financement du terrorisme (GCBF), “National Risk Assessment (NRA) : La corruption comme infraction préalable au blanchiment d’argent”, Avril 2019, <https://www.cdbf.ch/wp-content/uploads/2019/07/20190710_ber-korruption-geldwaescherei-f_final1.pdf> 1 June 2021.

the Agreement on the Swiss banks’ code of conduct with regard to the exercise of due diligence 1977

France

Autorite Des Marches Financiers, *'Guidelines on the obligation to report suspicious transactions to TRACFIN'* (2010).

European and international authorities

European Data Protection Supervisor, 'Preliminary Opinion on privacy by design', Opinion 5/2018 (31 May 2018) iii. <https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf> 10 June 2021.

Europol Report, 'From suspicion to action: Converting financial intelligence into greater operational impact' (2017), 22 <https://www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact> 1 June 2021.

Europol report, 'Does crime still pay? Criminal Asset Recovery in the EU - Survey of Statistical Information', European Police Office, 2016

Europol report, 'Why is cash still king: a strategic report on the use of cash by criminal groups as a facilitator for money laundering' European Police Office, 2015

FATF (20 June 2003), 'The Forty Recommendations' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf> 10 June 2021.

FATF (2016), Anti-money laundering and counter-terrorist financing measures - Switzerland, Fourth Round Mutual Evaluation Report, FATF, Paris, France, 162 <www.fatf-gafi.org/publications/mutualevaluations/documents/mer-switzerland-2016.html> 10 June 2021.

FATF (2018), Anti-money laundering and counter-terrorist financing measures – United Kingdom, Fourth Round Mutual Evaluation Report, FATF, Paris, France <http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-kingdom2018.html> 10 June 2021.

FATF (2020), Anti-money laundering and counter-terrorist financing measures - Switzerland, Enhanced Follow-up Report & 2nd Technical Compliance Re-Rating, FATF, Paris, 11 <http://www.fatf-gafi.org/publications/mutualevaluations/documents/fur-switzerland-2020.html>

FATF (June 1998), 'Financial Action Task Force on Money Laundering Annual Report 1997-1998', 10 <http://www.fatf-gafi.org/media/fatf/documents/reports/1997%201998%20ENG.pdf> 10 June 2021.

FATF (June 2010), 'FATF Report: Money Laundering through Money Remittance and Currency Exchange Providers' <https://rm.coe.int/fatf-report-money-laundering-through-money-remittance-and-currency-exc/16807150ad> 1 June 2021.

FATF (June 2013) 'FATF Guidance – Politically Exposed Persons (Recommendations 12 and 22)' <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf> 10 June 2021.

FATF, 'Guidance for A Risk-based approach - the banking sector' October 2014, 6 <http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf> 10 June 2021.

FATF, 'Money Laundering and Terrorism Financing 2004-2005 Typologies' Financial Action Task Force, Paris, 10 June 2005.

FATF, 'Operational Issues Financial Investigations Guidance', June 2012, 3.

FATF, The Forty Recommendations, 20 June 2003, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf> 10 June 2021.

FIU's In Action – 100 Cases from the Egmont Group (Weimin 2005), 173 (Case 15).

OECD, 'The Era of Bank Secrecy is over; The G20/OECD Process is Delivering Results', 26 October 2011, <https://www.oecd.org/ctp/exchange-of-tax-information/48996146.pdf> 10 June 2021.

Roger Vilkins AO, "The danger of driving both illicit markets and financial exclusion", remarks delivered at the 6th Annual International Conference on Financial Crime and Terrorism Financing, Kuala Lumpur, 8 October 2014, <http://www.fatf-gafi.org/publications/fatfgeneral/documents/danger-illicit-markets-financial-exclusion.html> 10 June 2021.

BOOKS

A Bacarese, K Levy and H Mulukutla, 'The management of information in the context of suspected money laundering cases' in B Rider (ed), *Research Handbook on International Financial Crime* (Edward Elgar Publishing 2015)

A Chandor, *The Penguin Dictionary of Computers* (Penguin books 1970)

A Gewirth, *Reason and Morality* (University of Chicago Press 1978)

A Steichen, 'Information Exchange in Tax Matters: Luxembourg's New Tax Policy' in A Rust and E Fort (eds), *Exchange of information and bank secrecy* (Kluwer Law International 2012)

B Corboz, *Les infractions en droit suisse*, (Berne, Volume II, 2010)

B Rider (ed), *Research Handbook on International Financial Crime* (Edward Elgar Publishing 2015)

B Unger, 'Money Laundering Regulation: from Al Capone to Al Qaeda' in B Unger and D vaan der Linde (eds), *Research Handbook on Money Laundering* (Edward Elgar 2013)

C Lombardini, *Banques et blanchiment d'argent* (3rd ed, Schulthess 2016)

C Lombardini, *Droit bancaire Suisse* (2eme ed, Schulthess 2008)

C S French, *Oliver and Chapman's Data Processing and Information Technology* (10th edn, Thomson 2004)

C Wells, *Corporations and Criminal Responsibility* (2nd ed, Oxford University Press 2001)

D Beyleveld and R Brownsword, *Law as a Moral Judgment* (Sheffield Academic Press 1994)

D Campbell (ed), *International Bank Secrecy* (Sweet & Maxwell 1992)

D Masciandaro, O Balakina, *Banking Secrecy: Economics and Politics* (Palgrave Macmillan 2015)

D Neo, 'A Conceptual Overview of Bank Secrecy' in S Booysen and D Neo (eds), *Can Banks Still Keep a Secret?: Bank Secrecy in Financial Centres Around the World* (Cambridge University Press 2017)

D Newcomb, B Burke and S Favretto 'USA' in G Godfrey and F Neate (eds), *Neate and Godfrey: Bank Confidentiality* (Bloomsbury Professional 2015)

D Ormerod and K Laird, *Smith, Hogan, and Ormerod's Criminal Law* (15th ed, OUP 2018)

D P Murphy, 'International developments surrounding the proceeds of crime (money laundering) and terrorist financing act' in *Dirty Money: civil and criminal aspects of money-laundering* - Conference Meredith Lectures 2002, Edition Tvon Blais, 2003.

D Poncet, A Macalusa, «Evolution de la responsabilité pénale de l'entreprise en Suisse et perspective inspirée de modèles étrangères», in *Strafrecht, Strafprozessrecht und Menschenrechte, Fetschrift fur Stefan Trechsel*, (Zurich 2002)

D Thurnherr 'The reception process in Austria and Switzerland' in H Keller and AS Sweet (eds), *A Europe of Rights: The Impact of the ECHR on National Legal Systems* (OUP 2008)

E F Malaspina, "History of International Law" in M Thommen *Introduction to Swiss law – Volume II* (Carl Grossmann Publishers 2018)

E Monfrini, 'The Abacha case' in M Pieth (ed), *Recovering Stolen Assets* (Peter Lang AG 2008)

E P Ellinger, E Lomnicka and C V M Hare, *Ellinger's modern banking law* (OUP 2011)

E U Savona, *Responding to money laundering – international perspectives* (Harwood academic publishers 1997)

F Gurry, *Breach of Confidence* (OUP 1998)

F Hobson, 'Introduction: Banks and Money Laundering' in W Blair and R Brent (eds), *Banks and Financial Crime: The International Law of Tainted Money* (OUP 2008)

F M Teichmann and B S Sergi, *Compliance in multinational corporations* (Emerald Publishing Limited 2018)

G Gilligan, 'Financial crime: a historical perspective' in B Rider (ed), *Research Handbook on International Financial Crime* (Edward Elgar Publishing 2015)

G Pavlidis, *Confiscation internationale: instruments internationaux, droit de l'Union Européenne, droit Suisse* (Schulthess 2012)

G Stessens, *Money Laundering – A new international law enforcement model* (Cambridge University Press 2000)

H Bollmann and P Gmuer, 'Switzerland' in D Campbell (ed), *International Bank Secrecy* (Sweet & Maxwell 1992)

H Fenwick and G Phillipson, *Media Freedom under the Human Rights Act* (OUP 2010)

H Keller and A S Sweet (eds), *A Europe of Rights: The Impact of the ECHR on National Legal Systems* (OUP 2008)

J Biggins, 'Dirty complexity: money laundering through derivatives' in B Unger and D van der Linde (eds) *Research Handbook on Money Laundering* (Edward Elgar Publishing 2013)

J Hull, *Commercial Secrecy: Law and Practice* (Sweet & Maxwell 1998)

J Kranacher, R Riley and J T Wells, *Forensic Accounting and Fraud Examination* (Wiley 2011)

J L Capdeville, *Le secret bancaire : étude de droit comparé (France, Suisse, Luxembourg) Tome 2* (PU Aix-Marseille 2006)

J Peddie, 'Investigations and remedies under POCA 2002', in W Blair, R Brent and T Grant (eds), *Banks and financial crime – the international law of tainted money* (2nd Edition, OUP 2017)

J Ulph, *Commercial Fraud : Civil Liability, Human Rights and Money Laundering* (OUP 2006)

K B Phelps and S Rhodes, *The Ponzi Book – A legal resource for unravelling ponzi schemes* (Matthew Bender Elite Products 2012)

K Hinterseer, *Criminal Finance – The political economy of money laundering in a comparative legal context* (Kluwer Law International 2002)

K Matthews, *Banks and the laundering of dirty money: The economics of money laundering* (Cardiff University, Discussion papers in Economics, August 2000)

K McCarthy, 'UK Part I: Laundering the proceeds of crime – Methodology?' in M Simpson, N Smith and A Srivastava (eds), *International guide to money laundering law and practice* (3rd edn, Bloomsbury Professional 2010)

L de Koker and M Turkington 'Anti-Money Laundering measures and the effectiveness question' in B Rider (ed) *Research Handbook on International Financial Crime* (Edward Elgar Publishing 2015)

M A Young, *Banking secrecy and offshore financial centers: Money laundering and offshore banking* (Routledge 2013)

M Harari, «Procédure pénale : la banque comme détentrice d'informations et de valeurs patrimoniales appartenant a son client» in L Thevenoz, C Bovet (eds), *Journée 2010 de droit bancaire et financier,*

M Hoffman, *Usury in Christendom: The Mortal Sin that Was and Now is Not* (Independent History and Research 2012)

M Levi, 'Foreword: some reflections on the evolution of economic and financial crime' in B Rider (ed), *Research Handbook on International Financial Crime* (Edward Elgar Publishing 2015)

M Levi, 'Money laundering and regulatory policies', in E U Savona, *Responding to money laundering – international perspectives* (Harwood academic publishers 1997)

M M Gallant, *Money laundering and the proceeds of crime – Economic crime and civil remedies*, (Edward Elgar 2005)

M N Jovanović, *The Economics of International Integration* (Edward Elgar 2006)

M Pieth, 'International standards against money laundering' in M Pieth and G Aiolfi (eds), *A Comparative Guide to Anti-Money Laundering* (Edward Elgar 2004)

M Richardson et al, *Breach of Confidence: Social Origins and Modern Developments* (Edward Elgar 2011)

M Sutherland Williams, M Hopmeier and R Jones, *Millington and Sutherland Williams on the Proceeds of Crime* (4th ed, OUP 2013)

M Yeandle et al, *Anti-Money Laundering Requirements : Costs , Benefits And Perceptions* (Z/Yen 2005)

M. Siems, *Comparative Law* (Cambridge University Press: 2014)

M. Zwick, *Banking Secrecy and Money Laundering* (Promoculture sarl 2003)

N Capus, 'Country Report: Combating money laundering in Switzerland' in M Pieth and G Aiolfi (eds), *A Comparative Guide to Anti-Money Laundering* (Edward Elgar 2004)

N Rouiller, *Droit suisse des obligations et Principes du droit européen des contrats* (Cedidac 2007)

N Ryder 'Introduction' in N Ryder (ed.) *White collar crime and risk – Financial crime, corruption and the financial crisis* (Palgrave Macmillan 2018)

O Abo Youssef and L Ruckstuhl "Switzerland" in *The international comparative legal guide to Anti-money laundering 2018* (Global Legal Group, 2018), [1.10] < https://iclg.com/practice-areas/anti-money-laundering-laws-and-regulations/switzerland> 20 January 2019.

O Audouin, La Lutte Anti Blanchiment dans la Banque (Afges 2007), 67

O Lajoix and M B Berlioz, 'France' in D Campbell (ed), *International Bank Secrecy* (Sweet & Maxwell 1992)

O Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015)

P Alldridge, *What Went Wrong with Money Laundering Law* (1st ed, Macmillan Publishers 2016)

P G Picht and G Studen, "Civil Law" in D Hurlimann and M Thommen (eds.), *Introduction to Swiss Law – Volume 2* (Carl Grossmann Publishers 2018)

R Brent, 'Regulatory Responsibilities' in W Blair, R Brent and T Grant (eds) *Banks and financial crime – the international law of tainted money* (2nd edn, OUP 2017)

R Cranston, *Principles of Banking Law* (Second edn, OUP 2002)

R Escobar and D Fisher, *The Accountant's Story: Inside the violent world of the Medellín cartel* (Grand Central Publishing 2009)

R Fortson QC, 'Money laundering offences under POCA 2002' in W Blair, R Brent and T Grant (eds), *Banks and financial crime – the international law of tainted money* (2nd edn, OUP 2017)

R P Meagher, J D Heydon, M J Leeming, *Meagher, Gummow and Lehane's equity, doctrines, and remedies* (4th edition, Sydney 2002)

R Parlour, 'Practicalities of Financial Crime Deterrence' in B Rider (ed), *Research Handbook on International Financial Crime* (Edward Elgar Publishing 2015)

R Pattenden, *The Law of Professional-Client Confidentiality* (Oxford University Press 2003)

R Schutze, *European Union Law* (2nd edn, Cambridge 2018)

R W Cahn, *The Coming of Materials Science* (Elsevier 2011)

R White and C Ovey, *Jacobs, White and Ovey: The European Convention on Human Rights*. (5th edn, OUP 2010)

S Besson, "The reception process in Ireland and the United Kingdom" in H Keller and AS Sweet (eds), *A Europe of Rights: The Impact of the ECHR on National Legal Systems* (OUP 2008)

S Breitenstein, 'Switzerland' in G Godfrey and F Neate (eds), *Neate and Godfrey: Bank Confidentiality* (Bloomsbury Professional 2015)

S Giroud and H Rordorf-Braun, *Droit suisse des sanctions et de la confiscation international* (Helbing Lichtenhahn Verlag 2020)

S Montagu-Cairns, 'Corporate criminal liability and the failure to prevent offence: an argument for the adoption of an omissions-based offence in AML' in K Benson, C King and C Walker (eds) *Assets, Crimes, and the State - Innovations in 21st Century Legal Responses* (Routledge 2020)

S Ogilvie and S Revell, 'International Anti-Money Laundering Initiatives' in G Godfrey and F Neate (eds), *Neate and Godfrey: Bank Confidentiality* (Bloomsbury Professional 2015)

S Savla, *Money Laundering and Financial Intermediaries* (Kluwer Law International 2001)

T Aplin et al., *Gurry on Breach of Confidence* (2nd ed, OUP 2012)

T Brooks, *Punishment* (Routledge 2012)

T Durner and L Shetret, 'Understanding bank de-risking and its effects on financial Inclusion (London: Oxfam 2015)

T Hartsch, "Switzerland", in M Simpson, N Smith and A Srivastava (eds) *International guide to money laundering law and practice* (3rd ed, Bloomsbury Professional 2010)

The international comparative legal guide to Anti-money laundering 2018 (Global Legal Group, 2018) < https://iclg.com/practice-areas/anti-money-laundering-laws-and-regulations/switzerland> 20 January 2019.

U Cassani, « Le blanchiment d'argent, un crime sans victim? » in N Schmid et al. (eds), *Wirtschaft und Strafrecht: Festschrift* (Schulthess 2001)

V Chadha, *Lifeblood of Terrorism: Countering Terrorism Finance* (Bloomsbury Publishing India 2015)

W Blair, R Brent and T Grant (eds), *Banks and financial crime – the international law of tainted money* (2nd edn, OUP 2017)

W C Gilmore, *Dirty Money: the evolution of money laundering measures to counter money laundering and the financing of terrorism* (3rd edn, Council of Europe Press 2004)

W Fowler and R Butler, 'Great Britain' in D Campbell (ed), *International Bank Secrecy* (Sweet & Maxwell 1992)

W H Muller, 'Anti-Money Laundering – A short story' in W H Muller, C H Kalin and J G Goldworth (eds), *Anti-money laundering – International law and practice* (John Wiley & Sons 2007)

W Trupman, 'The characteristics of economic crime and criminals' in B Rider (ed), *Research Handbook on International Financial Crime* (Edward Elgar Publishing 2015)

Y. Genier, *La fin du secret bancaire* (Savoir Suisse 2014)

Articles

‘The Thirteenth International Symposium on Economic Crime — Banking on Secrets: The Universal Balancing Act’, (1996) 3(3) J.F.C. 223.

‘Unofficial translation of the Swiss Federal Act on Banks and Savings Banks’ (KPMG, 1 January 2016)

“Financial Secrecy Index - 2018 Results” in the tax justice network’s website, <https://www.financialsecrecyindex.com/introduction/fsi-2018-results> 10 June 2021

“Financial Secrecy Index – 2020 Results” in the tax justice network’s website, <https://fsi.taxjustice.net/en/introduction/fsi-results> 10 June 2021.

A Antoine, « Les enjeux de la création d’une cour suprême au Royaume-Uni et la Convention de sauvegarde des droits de l’homme et des libertés fondamentales », (2008) 60(2) Revue internationale de droit comparé 283

A Conrad Hari, «Le blanchiment d’argent par omission» (2012) *RSDA* 361

A Donald, J Gordon and P Leach, “The UK and the European Court of Human Rights” (2012) 83 Equality and Human Rights Commission Research report, 156

A Jomini, « Présentation du Tribunal fédéral suisse comme autorité de juridiction constitutionnelle » Cahiers du Conseil Constitutionnel n° 18 (Dossier : Suisse) - Juillet 2005, <https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/presentation-du-tribunal-federal-suisse-comme-autorite-de-juridiction-constitutionnelle> 10 June 2021.

A Joshi, ‘In Pursuit of Big Data: An Analysis of International Funds Transfer Reporting’ RUSI Occasional Paper, April 2017, <https://rusi.org/sites/default/files/201704_rusi_in_pursuit_of_big_data_joshi.pdf> 10 June 2021.

A V M Leong, ‘Anti-money laundering measures in the United Kingdom: a review of recent legislation and FSA’s risk-based approach’ (2007) 28(2) Co Law 35

B Bertossa, « Confiscation et corruption, Quelques réflexions sur la confiscation des avantages obtenus par le corrupteur actif », SJ 2009 II, 379.

B Unger and F V Waarden, ‘How to Dodge Drowning in Data: Rule- and Risk-Based Anti Money Laundering Policies Compared” (2009) 5 Rev. L & Econ. 953

B. Schnyder, Code Civil (CC) in Dictionnaire Historique de la Suisse, version 18.11.2014 <http://www.hls-dhs-dss.ch/textes/f/F30734.php 1> 10 June 2021.

B. Wittes, “What Ben Franklin Really Said”, Lawfare Blog, 15 July 2011, <https://www.lawfareblog.com/what-ben-franklin-really-said> 10 June 2021.

C Balmat «Le GAFI en passe de criminaliser les délits fiscaux» *L’expert-comptable Suisse* 287

C F Green, ‘Business ethics in banking’ (1989) 8 *Journal of Business Ethics* 631

D Beyleveld and E Histed, ‘Betrayal of Confidence in the Court of Appeal’ (2000) 4 Med.L.Int. 277

D Beyleveld and S D Pattinson, ‘Horizontal applicability and horizontal effect’ (2002) 118 L.Q.R. 623

D Beyleveld, ‘The Principle of Generic Consistency as the Supreme Principle of Human Rights’ (2012) 13 Human Rts. Rev. 1

D Beyleveld, “The Concept of Human Right and Incorporation of the European Convention on Human Rights” (1995) P.L. 577

F Chaudet «L’obligation de diligence du banquier en droit privé» (1994) Swiss Law Review 20;

Federal Data Protection and Information Commissioner FDPIC, ‘The GDPR and its consequences for Switzerland’ March 2018

G Brown and T Evans, ‘The impact: the breadth and depth of the anti-money laundering provisions requiring reporting of suspicion activities’ (2008) Journal of International Banking Law Regulations 274

G E Sherman, ‘The Neutrality of Switzerland’ (1918) 12(2) The American Journal of International Law 241

G Greenleaf, ‘Global Data Privacy Laws 2019: 132 National Laws & Many Bills’ (2019) 157 *Privacy Laws & Business International Report* 14

G S Becker, ‘Crime and Punishment: An Economic Approach’ (1968) J. Pol. Econ. 76

H Fenwick and G Phillipson, ‘Confidence and privacy: A Re-examination’ (1996) 55 Cambridge L.J. 447

H R Steiner, M D Pfenninger, ‘Bank Confidentiality in Switzerland’ (1998) 1 JIBFL 14

J B Zufferey, C Lombardini, « L’obligation subsidiaire d’annonce et de dénonciation des ‘ORA LBA’ » (2007) *AJP* 1096

J Drage ‘Countering money laundering: the response of the financial sector’ (November 1992) B.E.Q.B. 2

J L Bacher, « Jurisprudence du TPF en matière de blanchiment d’argent: de gestion déloyale et d'escroquerie » (2011) *L’expert-comptable Suisse* 238

J T Kelly, ‘United States Foreign Policy: Efforts to penetrate bank secrecy in Switzerland from 1940 to 1975’ [1975] 6 Cal. W. Int'l L.J. 211

J von Bernstorff, ‘The Changing Fortunes of the Universal Declaration of Human Rights: Genesis and Symbolic Dimensions of the Turn to Rights in International Law’ (2008) 19(5) EJIL 903

J Wadsley, ‘Money laundering: professionals as policemen’ (1994) Conv. 275

K Eggenberger, ‘When is blacklisting effective? Stigma, sanctions and legitimacy: the reputational and financial costs of being blacklisted” [2018] 25(4) *Review of International Political Economy* 483

Kolly, « Le Tribunal fédéral Suisse », in the Tribunal Federal’s webpage <https://www.bger.ch/files/live/sites/bger/files/pdf/de/cahiers-cc_201606.pdf> 10 June 2021.

L Isaacs et al, ‘Impact of the Regulatory Environment on Refugees’ and Asylum Seekers’ Ability to Use Formal Remittance Channels’, July 2018, Knomad Working Paper 33, <https://www.knomad.org/sites/default/files/2018-07/KNOMAD_WP_Impacts%20of%20the%20Regulatory%20Environment%20on%20Refugees%e2%80%99%20and%20Asylum%20Seekers%e2%80%99%20Ability%20to%20Use%20Formal%20Remittance%20Channels.pdf> 10 June 2021.

L Wildhaber, ‘The European Convention on Human Rights and international law’ (2007) 56 International and Comparative Law Quarterly 217

M Akgun, ‘Turkey – financial institutions’ anti-money laundering/counter-terrorist financing duties and financial exclusion’ (April 2021) PL 445

M Goldby, ‘Anti-money laundering reporting requirements imposed by English law: measuring effectiveness and gauging the need for reform’ [2013] Journal of Business Law 367

M V Alstine, ‘The Universal Declaration and Developments in the Enforcement of International Human Rights in Domestic Law’, (2009) 24 Md. J. Int'lL 63

M Yeandle and M Wardle, ‘The Global Financial Centres Index 25 March 2019’, <https://www.longfinance.net/media/documents/GFCI_25_Report.pdf> 10 June 2021.

M. Akgun, ‘La réforme française du 13 Novembre 2014 sur le blocage administratif des sites internet provoquant au terrorisme ou en faisant l'apologie’ [2016] 25(7) TAAD 223,

M. Hirsig-Vouilloz « Le nouveau droit suisse de la confiscation pénale et de la créance compensatrice (art. 69 a 73 CP) » AJP 2007, 1376, Art 70 N9.

M. Hottelier, « Le contrôle de constitutionnalité des décisions de justice en Suisse ou l’exercice d’un contrôle concret des normes » <https://dice.univ-amu.fr/sites/dice.univ-amu.fr/files/public/122-hottelier.pdf> 6 June 2021.

M. Izorche « Propositions methodologiques pour la comparaison » (2001) 53(2) Revue internationale de droit compare, 289

N W Turner, ‘The Financial Action Task Force: International Regulatory Convergence through Soft Law’ (2014-2015) 59 N.Y. L. Sch. L. Rev. 547,

O Balakina, A D’Andrea and D Masciandaro, ‘Bank secrecy in offshore centres and capital flows: Does blacklisting matter?’ [January 2017] 32 *Review of Financial Economics* 30

O Dunant and M Wassmer, ‘Swiss Bank Secrecy: its Limits under Swiss and International Laws’ (1988) 20(2) Journal of International Law 543

O Pfersmann 'Le droit comparé comme interprétation et comme théorie du droit' (2001) 53(2) *Revue internationale de droit comparé* 278

P A Gallo and C C Juckes, ‘Threshold transaction disclosures: access on demand through latent disclosure rather than reporting’ (2005) 8(4) J.M.L.C. 328

P Fischer et al, «Développements actuels en droit pénal, fiscal et réglementaire : impacts significatifs sur la profession d’avocats» (2015) *Revue de l’avocat* 418

P He, ‘A typological study on money laundering’ (2010) 13(1) J.M.L.C. 15

P Marshall, ‘Does Shah v HSBC Private Bank Ltd make the anti-money laundering consent regime unworkable?’’ May 2010, Butterworths Journal of International Banking and Financial Law 287 (287-290)

P S Grassi and D Calvarese, 'The duty of confidentiality of banks in switzerland: where it stands and where it goes. Recent developments and experience. The swiss assistance to, and cooperation with the italian authorities in the investigation of corruption among civil servants in italy (the "clean hands" investigation): how much is too much? ' (1995) 7 Pace Int'l L.Rev. 333

P Yeoh, ‘Banks’ vulnerabilities to money laundering activities’ (2019) 23(1) J.M.L.C. 122

Préposé fédéral à la protection des données et à la transparence, «Nouvelle loi fédérale sur la protection des données: le point de vue du PFPDT» 9 février 2021.

Privacy International, ‘How financial surveillance in the name of counter-terrorism fuels social exclusion’ 2019 <https://www.privacyinternational.org/long-read/3257/how-financial-surveillance-name-counter-terrorism-fuels-social-exclusion> 10 June 2021.

S F Preller, ‘Comparing AML legislation of the UK, Switzerland and Germany, (2008) 11(2) J.M.L.C. 234

S Guex , 'The Origins of the Swiss Banking Secrecy Law and Its Repercussions for Swiss Federal Policy' (2000) 74 *Business History Review* 242.

S Lembo and C Hensler, ‘Whistleblowers in the Swiss Banking Sector: Legal Hurdles to Cooperating with Foreign Governments’ (Bär & Karrer Briefing, January 2015) <https://www.baerkarrer.ch/publications/BK%20Briefing_Whistleblowers%20in%20the%20CH%20Banking%20Sector.pdf> 10 June 2021.

S Nadelhofer Do Canto, « Quelques aspects de la confiscation selon l’art 70 al. 2 CP» RPS, 2008, 312.

S Ross and M Hannan, ‘Money laundering regulation and risk- based decision making’ (2007) 10(1) J.M.L.C. 106

T Finegan ‘Neither Dualism nor Monism: Holism and the Relationship between Municipal and International Human Rights Law’ (2011) 2(4) TLT, 477

Tax Justice Network, ‘Financial Secrecy Index 2018 - Narrative Report on the United Kingdom’, 2, <http://www.financialsecrecyindex.com/PDF/UnitedKingdom.pdf> 10 June 2021.

Tax Justice Network, ‘Financial Secrecy Index 2020 - Narrative Report on the United Kingdom’ , 2020, 1 <https://fsi.taxjustice.net/PDF/UnitedKingdom.pdf> .

Tax justice network, ‘Narrative Report on Cyprus – financial secrecy index 2020, <https://fsi.taxjustice.net/PDF/Cyprus.pdf> 10 June 2021

Tax justice network, ‘Narrative Report on Luxembourg – financial secrecy index 2020, <https://fsi.taxjustice.net/PDF/Luxembourg.pdf> 10 June 2021

Tax justice network, ‘Narrative Report on Switzerland – financial secrecy index 2018’, <https://www.financialsecrecyindex.com/PDF/Switzerland.pdf> 10 June 2021

Tax justice network, ‘Narrative Report on the Cayman Islands – financial secrecy index 2020’ <https://fsi.taxjustice.net/PDF/CaymanIslands.pdf> 10 June 2021.

The City UK,“Key facts about the UK as an international financial centre 2018” (The City UK, October 2018) https://www.thecityuk.com/assets/2018/Reports-PDF/94053cfc7b/Key-facts-about-the-UK-as-an-international-financial-centre-2018.pdf at 3

TheBanks.eu website, “Compare Countries By Banking Sector”, <https://thebanks.eu/compare-countries-by-banking-sector#ref_5> 10 June 2021.

UN, A/74/335 “Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism” <https://undocs.org/A/74/335> 10 June 2021

W de Capitani, ‘Banking secrecy today’ [1988] 10 U. Pa. J. Int'l. Bus. L. 57

THESIS

B Moutel, « L'Effet Horizontal de la Convention Européenne Des Droits de l'homme en Droit Privé Français: Essai sur la diffusion de la CEDH dans les rapports entre personnes privées » (PhD Thesis, l'Université de Limoges, 25 novembre 2006).

J. Cattan, « Le droit et les communications électroniques », (PhD Thesis, Aix-en-Provence 2012),

M Naim, «Eléments du droit comparé pour renforcer le secret bancaire» (PhD Thesis, Université Catholique de Louvain 1982), 231

R Stokes, 'The Banker's Duty of Confidentiality' (PhD thesis, University of Liverpool 2005),

S P Brown, 'The moral justification of retributive punishment by reference to the notion of balance' (PhD thesis, University of Sheffield 1998), 190.

WEBSITE

'Chinese wall', Corporate finance Institute website, <https://corporatefinanceinstitute.com/resources/knowledge/finance/chinese-wall-definition/> 10 June 2021

'Economic Declaration', Paris, 16 July 1989. <http://www.g8.utoronto.ca/summit/1989paris/communique/index.html> 10 June 2021.

'Howard Wilkinson', National Whistleblower Center, <https://www.whistleblowers.org/members/howard-wilkinson/> 10 June 2021; and

'Money – Laundering and Globalisation', UNODC website, <https://www.unodc.org/unodc/en/money-laundering/globalization.html> 10 February 2018.

'Offshore savers can kiss confidentiality goodbye' <https://www.telegraph.co.uk/finance/personalfinance/expat-money/8862417/Offshore-savers-can-kiss-confidentiality-goodbye.html> 10 June 2021,

'Spilling secrets: the end of confidentiality in offshore financial centres' <https://www.lexology.com/library/detail.aspx?g=b1668640-55d0-4627-b95f-7999047328d4> 10 June 2021.

"Money Laundering", Interpol web site, <https://www.interpol.int/Crime-areas/Financial-crime/Money-laundering> accessed 14 June 2018.

"Special Future- Money Laundering" (UN Special Futures, UN General Assembly Special Session on the World Drug Problem 8-10 June 1998) <https://www.un.org/ga/20special/featur/launder.htm> 18 December 2018.

"Venezuelan Billionaire News Network Owner, Former Venezuelan National Treasurer and Former Owner of Dominican Republic Bank Charged in Money Laundering Conspiracy Involving Over $1 Billion in Bribes", Department of Justice Office of Public Affairs, Justice News, 20 November 2018,

<https://www.justice.gov/opa/pr/venezuelan-billionaire-news-network-owner-former-venezuelan-national-treasurer-and-former> 23 December 2018.

A Haefliger, «Le Tribunal Fédéral Suisse » in Annuaire international de justice constitutionnelle – La hiérarchie des normes constitutionnelles et sa fonction dans la protection des droits fondamentaux, Le principe de non-rétroactivité des lois 1990, 6, 195, 195-196. <https://www.persee.fr/doc/aijc_0995-3817_1992_num_6_1990_1131> 10 June 2021.

AMLA 1997's unoffical English translation available at the Federal Council's website: <https://www.fedlex.admin.ch/eli/cc/1998/892_892_892/en> 10 June 2021

Chicago Inspector General Joe Ferguson, video in <https://news.wttw.com/2019/01/30/inspector-general-decries-keep-your-mouth-shut-culture-city-hall> 10 June 2021.

Executive Order 13224 of 2001 (2001), <http://georgewbush-whitehouse.archives.gov/

F Coppola, 'The Banks That Helped Danske Bank Estonia Launder Russian Money', Forbes, Sep 30, 2018, <https://www.forbes.com/sites/francescoppola/2018/09/30/the-banks-that-helped-danske-bank-estonia-launder-russian-money/#3defa2207319> 10 June 2021.

F Keating, "Gangs force thousands of teens to become 'money mules'", Independent, 29 July 2017 <https://www.independent.co.uk/news/uk/teenagers-money-laundering-money-mules-criminal-gangs-gangsters-criminals-fraud-a7866151.html> 10 June 2021.

FATF website, 'High-risk and other monitored jurisdictions', <http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/more/more-on-high-risk-and-non-cooperative-jurisdictions.html?hf=10&b=0&s=desc(fatf_releasedate)> 10 June 2021.

FATF website, "Outcomes FATF Plenary, 21-23 February 2018" <http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-february-2018.html> 10 June 2021.

Federal Office of Police website, "Art. 305ter para. 2 SCC – right to report a mere suspicion" <https://www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/geldwaescherei/meldung/meldeformular/art_305_stgb.html> 10 June 2021.

ICO website, "What is personal data?" <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/> 10 June 2021.

ICO website, What ist the meaning of 'relates to'? <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-the-meaning-of-relates-to/> 10 June 2021.

J Garside, "Is money-laundering scandal at Danske Bank the largest in history?" The Guardian, 21 September 2018, <https://www.theguardian.com/business/2018/sep/21/is-money-laundering-scandal-at-danske-bank-the-largest-in-history> 13 October 2018

J Thomas, 'Money laundering in the 21st century: Follow the money' Payments Cards & Mobile website <http://www.paymentscardsandmobile.com/money-laundering-in-the-21st-century/> 9 June 2021.

J Thomas, 'Money laundering in the 21st century: Follow the money' Payments Cards & Mobile website <http://www.paymentscardsandmobile.com/money-laundering-in-the-21st-century/> 9 June 2021.

L Caflisch, « La pratique suisse en matière de droit international public » Département fédéral des affaires étrangères, 2013, 6, <https://www.eda.admin.ch/dam/eda/fr/documents/das-eda/organisation-eda/130425-RSDIE-pratique-2011-complet_fr.pdf> 6 June 2021.

M Martini, “Need help laundering money? What about buying your own bank?” Transparency Inernational Medium, 4 December 2018, < https://voices.transparency.org/need-help-laundering-money-what-about-buying-your-own-bank-5127457f09a8> 21 December 2018.

M Smith, S Valle and B. Schmidt, ‘No One Has Ever Made a Corruption Machine Like This One’ Bloomberg Businessweek, 8 June 2017, <https://www.bloomberg.com/news/features/2017-06-08/no-one-has-ever-made-a-corruption-machine-like-this-one> 30 June 2021.

Masak website, Örnek davalar available <http://www.masak.gov.tr/tr/content/aklama-yontemleri/59> 10 June 2021.

Ministry of Justice, Corporate Liability for Economic Crime Call for evidence, January 2017, <https://consult.justice.gov.uk/digital-communications/corporate-liability-for-economic-crime/supporting_documents/corporateliabilityforeconomiccrimeconsultationdocument.pdf> 10 June 2021 .

N Cori, « Paradis fiscaux : Sarkozy rêve tout haut » Libération, 25 septembre 2009, <http://www.liberation.fr/france/2009/09/25/paradis-fiscaux-sarkozy-reve-tout-haut_583849> 10 June 2021.

N Faith and A Macleod, ‘The mysterious private banks of Geneva, Euromoney, <https://www.euromoney.com/article/b1d06hwcxgbq9y/the-mysterious-private-banks-of-geneva> 10 June 2021.

NCA’s website, ‘SAR Quality Issues,: <https://www.ukciu.gov.uk/(b04b1m2pl1jooaqcnqutd3qe)/Information/info.aspx?InfoSection=Quality> 10 June 2021.

news/releases/2001/09/print/20010924-1.html> 1 October 2018.

Oxford English Dictionary, <http://www.oed.com/view/Entry/95568?redirectedFrom=information#eid> 10 June 2021

Plea Agreement, United States of America against Odebrecht S.A. (Cr. No. 16-643 (RID)) <https://www.justice.gov/opa/press-release/file/919916/download> 19 December 2017

R U Vogler, ‘History’ in Swiss Bankers Association’s website. An extract taken from the “100 years of Swiss Banking. 100 people. 100 thank you”, published for the 100th birthday of the SBA. <https://www.swissbanking.org/en/bankers-association/about-us/history> 10 June 2021.

Recovering the Proceeds of Crime (Performance Innovation Unit, Cabinet Office, June 2000).

The Federal Council’s website, Unofficial translation of Swiss Criminal Code of 21 December 1937, <https://www.admin.ch/opc/en/classified-compilation/19370083/index.html> 20 January 2020

UN treaties website, <https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=VI-19&chapter=6&clang=_en> and <https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html> accessed 30 September 2021.

UNODC website, “Money – Laundering and Globalisation” <https://www.unodc.org/unodc/en/money-laundering/globalization.html> 10 June 2021.

Unoffical translation of Federal Act of 10 October 1997 on Combating Money Laundering and Terrorist Financing in the Financial Sector in the Federal Council’s website: <https://www.fedlex.admin.ch/eli/cc/1998/892_892_892/en> 10 June 2021.

Unofficial translation of Penal Code, With the participation of John Rason Spencer QC, prepared in 1995 and updated 2005, 57 <https://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations> 21 January 2021.

Webpage of the popular initiative «Oui à la protection de la sphère privée»: <http://www.proteger-la-sphere-privee.ch/> 3 May 2020.

Z Rodionova, 'London property market turned into money laundering safe haven by inadequate supervision, MPs say', The Independent, 15 July 2016 <https://www.independent.co.uk/news/business/news/london-property-market-real-estate-money-laundering-overseas-foreign-buyers-mps-a7138176.html> 10 June 2021

enforcement of the clauses would be contrary to public policy.[16] The appeal was dismissed.

Kershwyn Bassuday
Lecturer, *Commercial Law Department, University of Cape Town*

Turkey—Financial institutions' anti-money laundering/counter-terrorist financing duties and financial exclusion

LT Bankers' duties; Due diligence; Money laundering; Prevention of terrorism; Terrorist financing; Turkey

The Financial Action Task Force (FATF) sets universally recognised international standards for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.[1] The FATF's recommendation 10 advises countries to impose by enforceable means on financial institutions a duty to undertake initial (i.e. before establishing business relations) and on-going customer due diligence measures. According to the recommendation, where the financial institution is unable to comply with the applicable customer due diligence requirements, "it should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship".[2] Moreover, the FATF adopted a risk-based approach. A risk-based approach to anti-money laundering/counter-terrorist financing (AML/CFT) for banks means that they

> "are expected to identify, assess and understand the money laundering and terrorist financing risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively."[3]

The general principle of a risk-based approach is that

> "where there are higher risks, relevant persons should take enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are lower, simplified measures may be permitted."[4]

Taking into account financial institutions' duty to undertake customer due diligence measures as well as other AML/CTF duties, some authors argue that financial institutions have become the private police force of the financial sphere.[5]

[16] *Beadica* [2020] ZACC 13 at [96].

[1] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations* (Paris: FATF, 2012–2020), p.7, *http://www.fatf-gafi.org/recommendations.html* [Accessed 18 January 2021].

[2] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations* (2020), Recommendation 10, "Customer due diligence".

[3] Financial Action Task Force, *Guidance for A Risk-based approach—the banking sector* (Paris: FATF, 2014), p.6, *http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf* [Accessed 18 January 2021].

[4] Financial Action Task Force, Interpretive Note to Recommendation 1, "Assessing risks and applying a risk-based approach".

[5] e.g. Joan Wadsley, "Money laundering: professionals as policemen" [1994] Conv. 275, 276.

However, financial institutions that are required to undertake customer due diligence measures in a risk-sensitive manner are profit-oriented entities, and undertaking such measures costs money. Accordingly, there have been a number of cases in different jurisdictions which indicate that that, where enhanced due-diligence measures would be required, financial institutions sometimes simply refuse applications to open bank accounts.[6] The FATF also recognised in its 2016 report that some financial institutions prefer terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage money laundering and terrorist financing risk (i.e. de-risking or de-banking).[7] De-banking leads to unjustifiable financial exclusion of some categories of people, in particular of low-profit customers such as refugees and some expatriates, and interference with the exercise of their rights and freedoms.[8]

A recent and interesting example of financial exclusion came from Turkey. Mr Gergerlioğlu, a member of the Turkish Parliament, asked written questions to the Vice-President of the Republic of Turkey regarding allegations that financial institutions had refused to open bank accounts for former state officials who had been dismissed as a result of state of emergency decrees.[9] Government representatives implicitly accepted the allegations and defended, in a one sentence long written answer, that relevant decisions of the banks are in compliance with applicable banking law and AML/CTF law rules. The decrees in question provided for dismissal of over 100,000 state officials, following an attempted coup in 2016, on the ground that they had been members of, or had connections with, terrorist organisations or organisations listed by the National Security Council. It is worth mentioning that state of emergency decrees are governmental decrees, not judicial decisions, and these decrees do not prohibit listed officials from opening a bank account or making financial transactions. Nevertheless, on the basis of these decrees, financial institutions may conclude that listed former state officials are medium- or high-risk customers, in respect of whom enhanced customer due diligence measures would be required. As in other jurisdictions, it seems that they preferred to reject applications rather than to incur these additional costs. The consequence has been that former officials who have been denied a bank account

[6] e.g. In relation to financial exclusion of refugees, see L. Isaacs et al, *Impact of the Regulatory Environment on Refugees' and Asylum Seekers' Ability to Use Formal Remittance Channels* (Knomad, 2018), Knomad Working Paper 33, pp.21–23, *https://www.knomad.org/sites/default/files/2018-07/KNOMAD_WP_Impacts%20of%20the%20Regulatory%20Environment%20on%20Refugees%e2%80%99%20and%20Asylum%20Seekers%e2%80%99%20Ability%20to%20Use%20Formal%20Remittance%20Channels.pdf* Accessed 18 January 2021]. In relation to foreigners who were denied bank accounts in Bulgaria after the adoption of the Law Book (the provision on the application of the norms) to the Law on Measures against Money Laundering, see "What are the recent problems with opening bank accounts for foreigners in Bulgaria?" (*Euroformat*, 5 November 2019), *http://blog.euroformat.eu/what-are-the-recent-problems-with-opening-bank-accounts-for-foreigners-in-bulgaria/roformat.eu*. In relation to the US citizens residing overseas who were denied of bank accounts in the US after the US Patriot Act, see Association of Americans Resident Overseas, "Americans Residing Overseas are Denied Bank Accounts", *https://aaro.org/38-position-papers-2009/22-position-americans-residing-overseas-are-denied-bank-accounts-2009* [Accessed 18 January 2021].

[7] Financial Action Task Force, *Guidance on correspondent banking services* (Paris: FATF, 2016), p.4, *https://www.fatf-gafi.org/publications/fatfrecommendations/documents/correspondent-banking-services.html* [Accessed 18 January 2021].

[8] T. Durner and L. Shetret, *Understanding Bank De-Risking and Its Effects on Financial Inclusion* (London: Oxfam, 2015), p.9, *https://www.oxfam.org/sites/www.oxfam.org/files/file_attachments/rr-bank-de-risking-181115-en_0.pdf*.

[9] Written questions by Ö.F. Gergerlioğlu, No:7/24544 (28/01/2020); No:7/24745 (28/01/2020); No:7/31508 (24/06/2020).

have faced problems in finding jobs, making payments, such as for rent and other necessities, and making investments.[10]

Thanks to media coverage of this problem, it has been reported that some banks have changed their decisions and have now opened bank accounts for dismissed officials.[11] However, the possibility remains that similar decisions could be taken in future. It is therefore suggested that financial institutions' AML/CTF duties need to be redesigned to ensure that they take into account the impact of their decisions on the rights and freedoms of existing and prospective clients and not merely their own financial interests.

Mustafa Akgün
PhD candidate, *Durham Law School*

[10] Ö.F. Gergerlioğlu submitted that some have lost their job only because they were not able to open a bank account to be paid: "Bankaların hesap açmadığı KHK'liler işlerinden oluyor" (*Evrensel*, 27 January 2020), *https://www.evrensel.net/haber/396124/bankalarin-hesap-acmadigi-khkliler-islerinden-oluyor* [Accessed 18 January 2021].

[11] e.g. "Garanti Bankası tepkiler sonrası KHK'lı müşteriye sınırlamaları kaldırdı, özür diledi" (*Euronews*, 9 January 2020), *https://tr.euronews.com/2020/01/09/garanti-bankasi-tepkiler-sonrasi-khk-li-musteriye-sinirlamalari-kaldirdi-ozur-diledi* [Accessed 18 January 2021]; B. Karakas, "Bankadan KHK yanıtı: Kartı ihraç nedeniyle kapatıldı" (Deutsche Welle Türkçe, 7 May 2020), *https://www.dw.com/tr/bankadan-khk-yan%C4%B1t%C4%B1-kart%C4%B1-ihra%C3%A7-nedeniyle-kapat%C4%B1ld%C4%B1/a-53363760* [Accessed 18 January 2021].

improving the representation of women in elected office, and Samoa's experience will be examined by others in the Pacific and beyond. The irony in Samoa is that the operation of the quota may deny FAST's leader, Fiame Naomi Mata'afa, a place in history as Samoa's first female Prime Minister.

Anna Dziedzic
Global Academic Fellow, University of Hong Kong Faculty of Law

Turkey and Switzerland—Legal confidentiality and lawyers' duty of making suspicious transaction reports

keywords to be inserted by the indexer

The Financial Action Task Force (FATF) is an inter-governmental body producing non-binding recommendations to set global standards for combating money laundering and terrorist financing.[1] The FATF advises countries to take measures increasing law enforcement agencies' capacity to detect illicit money.[2] One of these measures is imposing upon financial institutions and designated non-financial businesses and professions a duty to produce suspicious transaction reports (STRs) where they suspect, or have reasonable grounds to suspect, that funds are the proceeds of criminal activity, or are related to terrorist financing.[3] According to the FATF's recommendation 23, the duty of reporting should extend to lawyers when, on behalf of or for a client, they engage in a financial transaction in relation to one of the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.[4]

Most Member States of the Council of Europe implemented recommendation 23 and imposed upon lawyers a duty of reporting. Anti-money laundering/counter-terrorist financing laws that impose on lawyers a duty to produce suspicious transaction reports were subject to European Court of Human Rights' examination in *Michaud v France*. Mr Michaud, a lawyer registered to the Paris Bar, argued that requiring lawyers to report their suspicions would infringe individual freedom and the smooth functioning of justice because confidentiality between lawyer and client is of crucial importance in the practice of the legal

[1] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations* (Paris: FATF, 2012–2020), p.7, *http://www.fatf-gafi.org/recommendations.html* [Accessed 9 July 2021].
[2] e.g., see Financial Action Task Force, *The FATF Recommendations* (2020), recommendations 10–16, 20–23 and 29–31, pp.14–25.
[3] Financial Action Task Force, *The FATF Recommendations* (2020), recommendations 20–23, pp.19–21.
[4] Financial Action Task Force, *The FATF Recommendations* (2020), recommendations 22 and 23, pp.19–21.

profession.[5] Bar associations also opposed the extension of the duty of reporting to lawyers, arguing that forcing lawyers to investigate their clients' financial transactions and informing public authorities of their clients' suspicious transactions, threatened the essential values of the legal profession. The Council of Bars and Law Societies of Europe submitted that the duty of reporting undermines the independence of lawyers, professional secrecy and people's right to respect for their private life, by making the lawyer a de facto agent of the state, entering into a conflict of interest with their clients.[6] The European Bar Human Rights Institute defended that professional confidentiality is an absolute duty of the lawyer in all their activities and in respect of all their files.[7]

Article 8 of the European Convention on Human Rights includes a right to professional confidentiality.[8] Therefore, imposing upon lawyers a duty of filing STRs relating to their client's financial affairs may interfere with the right to privacy as recognised in art.8 of the Convention. The European Court of Human Rights has established that:

> "Article 8 … affords strengthened protection to exchanges between lawyers and their clients. This is justified by the fact that lawyers are assigned a fundamental role in a democratic society, that of defending litigants. Yet lawyers cannot carry out this essential task if they are unable to guarantee to those they are defending that their exchanges will remain confidential."[9]

Lawyer-client relationships are not the only professional relation to which art.8 affords strengthened protection. The court established, for instance, that art.8 affords strengthened protection to the relation between the doctor and patient.[10] Judge de Meyer defended in *Z v Finland* that:

> "[W]hatever the requirements of criminal proceedings may be, considerations of that order do not justify disclosing confidential information arising out of the doctor/patient relationship or the documents relating to it."[11]

The Strasbourg Court has not followed Judge de Meyer's position in either medical confidentiality or legal confidentiality related cases.[12] The European Court held in *Michaud* that requiring lawyers to report suspicious transactions did not amount to excessive interference with the right to privacy. Two factors were decisive in the eyes of the court in assessing the proportionality of the interference. First, lawyers were not subjected to the duty of reporting where the activity in question related to active judicial proceedings. Secondly, law-makers had taken further measures to protect lawyers' professional privilege where the lawyer was subjected to the duty of reporting. For instance, lawyers were not supposed to transmit reports

[5] *Michaud v France* (2014) 59 E.H.R.R 9 at [63].

[6] Written comments submitted by the Council of Bars and Law Societies of Europe, *Michaud v France* (2014) 59 E.H.R.R 9 at [75].

[7] Written comments submitted by the European Bar Human Rights Institute, *Michaud v France* (2014) 59 E.H.R.R 9 at [86]. For a similar argument defended by the Council of Bars and Law Societies of Europe, see Written comments (n7).

[8] See *Niemietz v Germany* (1993) 16 E.H.R.R. 97 at [28]; and *Wieser and Bicos Beteiligungen GmbH v Austria* (2008) 46 E.H.R.R. 54 at [65].

[9] *Michaud v France* (2014) 59 E.H.R.R 9 at [118].

[10] *Z v Finland* (1998) 25 E.H.R.R. 371 at [96].

[11] *Z v Finland* (1998) 25 E.H.R.R. 371, partly dissenting opinion of Judge De Meyer at [I].

[12] *Z v Finland* (1998) 25 E.H.R.R. 371 at [144] and [145]; *Michaud v France* (2014) 59 E.H.R.R 9 at [120]; *Altay v Turkey* (2020) 70 E.H.R.R. 4 at [52].

directly to the police authorities but to some elected lawyers at the Bar of which the lawyer was a member. This meant that some senior lawyers at the Bar were expected to act as a filter protecting lawyers' professional privilege.[13]

Anti-money laundering/counter-terrorist financing laws imposing a duty of reporting on lawyers have lately been subject to a vivid debate in two Member States of the Council of Europe: Turkey and Switzerland. The Turkish Parliament extended the duty of suspicious activity reporting to lawyers on 27 December 2020. The Swiss Parliament rejected on 1 March 2021 a Bill imposing on lawyers a duty of reporting.

The FATF officials, in the *Mutual Evaluation Report* of 2019, criticised Turkish law for not imposing upon lawyers a duty of reporting.[14] One year after the release of the report, the extension of the duty of suspicious transaction reporting to lawyers was proposed in a Bill dated 16 December 2020.[15] 72 out of 80 Bars in Turkey published a declaration on 24 December 2020 where they opposed the proposition, defending that the legal profession was indivisible and lawyers could not be forced to breach their clients' secrecy.[16] The Turkish Parliament, however, adopted the Bill on 27 December 2020 and extended the duty of reporting recognised in Law No.5549 to lawyers.[17] The only measure Turkish legislators took to protect lawyers' professional privilege was that, where the activity in question related to active judicial proceedings, the lawyer was not under duty to make an STR.

The FATF officials criticised Switzerland for not imposing upon lawyers a duty of reporting.[18] The Swiss Federal Council proposed on 26 June 2019 revision of the Anti Money Laundering Act 1997 to extend the duty of suspicious activity reporting to lawyers.[19] Imposing upon lawyers a duty of reporting had been the most discussed subject at all stages of the Bill.[20] The Swiss Bar Association opposed the proposition, defending that the legal profession was indivisible and legal privilege was absolute.[21] On 1 March 2021, the Swiss Parliament rejected imposing upon lawyers a duty of reporting.[22]

The examples of Turkey and Switzerland show that imposing upon lawyers a duty of reporting is subject to a debate in countries that had not yet given full effect to the FATF's recommendation 23. In fact, this issue is subject to a debate in countries that have already recognised lawyers' duty of reporting. For instance, the Law Commission of England and Wales in 2019 criticised the defensive

[13] *Michaud v France* (2014) 59 E.H.R.R 9 at [127], [129].

[14] Financial Action Task Force, *Anti-money laundering and counter-terrorist financing measures—Turkey, Fourth Round Mutual Evaluation Report* (Paris: FATF, December 2019), pp.201–202, *http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-turkey-2019.html* [Accessed 9 July 2021].

[15] Kitle İmha Silahlarının Yayılmasının Finansmanının Önlenmesine İlişkin Kanun Teklifi, 27/4; 2/3261.

[16] "Avukatlığın Özüne Aykırı Bu Düzenleme Kabul Edilemez" (*Istanbul Barosu*, 24 December 2020), *https://istanbulbarosu.org.tr/HaberDetay.aspx?ID=16115* [Accessed 9 July 2021].

[17] Law No.7262, adopted on 27 December 2020.

[18] Financial Action Task Force, *Anti-money laundering and counter-terrorist financing measures—Switzerland, Fourth Round Mutual Evaluation Report* (Paris: FATF, 2016), p.238, *https://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-switzerland-2016.html* [Accessed 9 July 2021].

[19] FF 2019 5237, pp.5252–5258.

[20] *Dépêche ATS, Délibérations au Conseil national*, *https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20190044* [Accessed 9 July 2021]

[21] "Avant-projet du 1 juin 2018 de modification de la loi fédérale concernant la lutte contre le blanchiment d'argent et le financement du terrorisme", "Thema/Question du jour", *Anwalts Revue de l'Avocat*, 10/2018, pp.414–416, *https://www.sav-fsa.ch/fr/documents/dynamiccontent/03arv1018.pdf* [Accessed 5 May 2021].

[22] *Conseil national, Session de printemps 2021, Première séance*, 1 March 2021 14h30, 19.044, *Vote sur l'ensemble namentliche-nominatif*, 19.044/22277.

over-reporting culture existing amongst reporting persons, including lawyers.[23] Where lawyers make unwarranted disclosures, this would irreversibly affect individuals' trust in lawyers and, therefore, would deeply affect the smooth functioning of justice. Therefore, it is submitted that the lawyers' duty to produce STRs should be re-investigated considering Judge de Meyer's dissenting opinion in *Z v Finland*, where he defended the possibility of a duty of confidentiality which could not be limited for the prevention and prosecution of crime.

Mustafa Akgün
PhD Candidate, *Durham Law School*

United States of America—Supreme Court Term 2020 Overview

keywords to be inserted by the indexer

California v Texas rejects challenge to the Affordable Care Act's "minimum essential coverage" provision. *Brnovich v Democratic National Committee* upholds two Arizona election laws. *Fulton v City of Philadelphia* upholds Catholic foster care agency's right to reject referrals to same-sex and unmarried couples. *National Collegiate Athletic Association v Alston* mandates modest expansion of education-related benefits to students. *Tenzin v Tanvir* greenlights suits against FBI agents after Muslims were placed on the "no-fly" list in retaliation for their refusal to serve as government informants.

The October 2020 term of the United States Supreme Court featured fewer decisions rendered by a closely-divided court than in previous terms. I refer the reader to Scotusblog for statistics.[1] The lowest rate of agreement between any two justices (in the 56 cases decided with merit opinions) was 57 per cent. This rate was scored to Sotomayor and Alito JJ. These justices modestly improved their 49 per cent rate of agreement from October term 2019. The historical statistics supplying this metric (and many others) will be found under the tab "Stat Pack".

In *Texas v California* the Supreme Court rejected the third challenge to the Affordable Care Act (ACA) (Obamacare).[2] Breyer J wrote for the court. Thomas J concurred. Alito J dissented, joined by Gorsuch J. In 2017, Congress reduced the penalty for taxpayers who failed to purchase "minimum essential coverage" through private insurance markets.[3] It set the rate to zero. After 2017, Breyer J concluded, the ACA inflicted no injury on them. Texas (and other plaintiff states) argued that state financial burdens (they shouldered under the ACA) would increase. Breyer J also concluded that the state plaintiffs lacked standing: (a) reliance on third-party decision-making (such as an individual's decision to enroll in Medicaid) rendered injury to the state plaintiffs conjectural; and (b) the burdens (imposed by

[23] Law Commission of England and Wales, *Anti-money laundering: the SARs regime* (TSO, 2019), HC 2098, Law Com. No.384, para.5.12, *https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2019/06/6.5569_LC_Anti-Money-Laundering_Report_FINAL_WEB_120619.pdf* [Accessed 9 July 2021].

[1] See *https://www.scotusblog.com/statistics/* [Accessed 9 July 2021]. I refer to the "Justice Agreement" tab.

[2] *Texas v California* (2021) 141 S. Ct. xxxx; 945 F. 3d 355 reversed and remanded.

[3] See Tax Cuts and Jobs Act of 2017, Pub. L. 115–97, Sec. 11081, 131 Stat. 2092, codified at 26 USC s.5000A(c).