Ethics and good governance for public-private partnerships in the framework of countering financial crime: 10 recommendations

March 2023 | Maja Dehouck

University of Amsterdam

Project craaft
Collaboration, Research & Analysis Against the Financing of Terrorism

This project was funded by the European Union's Internal Security Fund – Police

Ethics and good governance for public-private partnerships in the framework of countering financial crime: 10 recommendations

Author: Maja Dehouck (M.Sc., LL.M.)
P.I.: Prof. dr. Marieke de Goede

Amsterdam Institute for Social Science Research
m.r.j.dehouck@uva.nl

Published in March 2023 by the University of Amsterdam

University of Amsterdam

Project craaft
Collaboration, Research & Analysis Against the Financing of Terrorism

This project was funded by the European Union's Internal Security Fund – Police

About

This report is part of a three-year research project on the ethical and legal challenges associated with public-private financial information-sharing. The project is being carried out at the Amsterdam Institute for Social Science Research of the University of Amsterdam, as part of Project CRAAFT.

Project CRAAFT (Collaboration, Research & Analysis Against the Financing of Terrorism) is an academic research and community-building project designed to build stronger, more coordinated efforts to combat the financing of terrorism across the European Union (EU) and in its neighbourhood. The project engages with authorities and private entities in order to promote cross-border connections and targeted research.

Funded by the EU Internal Security Fund – Police, the project is being implemented by a consortium led by RUSI Europe, along with the University of Amsterdam, Bratislava-based think tank GLOBSEC, and the International Centre for Counter-Terrorism (ICCT), based in The Hague. For more information, see: https://www.projectcraaft.eu/

About the author

Maja Dehouck is a researcher and PhD Candidate at the Department of Political Science at the University of Amsterdam. She holds an LLM in International and European Law and an MSc in Social and Cultural Anthropology. Her areas of research include anti-financial crime and the trade in cultural goods.

This research was carried out under the supervision of Prof. dr. Marieke de Goede, Professor of Political Science and Dean of the Faculty of Humanities at the University of Amsterdam. She has nearly 20 years of experience in research on the way in which financial data are used in counter-terrorism and security practices. She is the author of 'Speculative Security: the Politics of Pursuing Terrorist Monies' (University of Minnesota Press) and was Principal Investigator of Project FOLLOW: Following the Money from Transaction to Trial (www.projectfollow.org).

Acknowledgements

Our sincere gratitude goes out to those who provided feedback on earlier versions of this report. Special mention goes to the participants in the Expert Roundtable on October 8th, 2022: David Artingstall, Dr. Rocco Bellanova, Dr. Esmé Bosma, Magdalena Brewczyńska, Valeria Ferrari, Dr. Catherine Jasserand-Breeman, Dr. Pieter Lagerwaard, Lennaert Peek, Stephen Reimer, Lia van Broekhoven and Dr. Mara Wesseling. We would also like to thank all interviewees for their participation in this research, as well as Project CRAAFT consortium partners Tom Keatinge, Dr. Kinga Redlowska and Stephen Reimer from RUSI and RUSI Europe for the project support and for facilitating access to interview contacts and field sites.

Contents

Executive summary 5

List of abbreviations 7

1. Introduction 9

1.1 Study objectives and research questions 10

1.2 Scope 10

1.3 Methodology 11

1.4 Structure of this report 12

2. Case studies: findings 13

2.1 The Netherlands 13
2.1.1 Financial information-sharing in the Netherlands 13
2.1.2 Terrorism Financing Task Force 15

2.2 Sweden 23
2.2.1 Financial information-sharing in Sweden 23
2.2.2 SAMLIT 25

2.3 Canada 36
2.3.1 Financial information-sharing in Canada 36
2.3.2 Canadian PPPs 37

2.4 United Kingdom 42
2.4.1 Financial information-sharing in the UK 42
2.4.2 JMLIT 42

3. Ethics and PPPs: Recommendations 51

Recommendation 1: Re-evaluate the place of PPPs in the broader AML/CFT architecture 51

Recommendation 2: Investigate and mitigate the vulnerabilities of PPPs being used for illegitimate purposes 52

Recommendation 3: Align operations with good governance objectives and ethical principles 53

Recommendation 4: Establish a solid legal basis prior to the onset of activities 54

Recommendation 5: Limit tactical information sharing to proportionate use 55

Recommendation 6: Preserve the privacy and data protection rights of citizens 56

Recommendation 7: Enhance transparency of PPPs 58

Recommendation 8: Systematically evaluate the impact of PPPs 59

Recommendation 9: Task dedicated agencies with oversight of PPPs and ensure that PPPs are held accountable 60

Recommendation 10: Ensure that citizens can exercise their rights where they are affected by PPPs 61

4. Conclusion 62

Annex 1: Sources cited 63

Annex 2: Data collection 69

Executive summary

This study contributes to a better understanding of public-private financial information-sharing partnerships (PPPs) in the framework of preventing and fighting financial crime, by raising awareness of their ethical aspects. This report is divided into two parts. It firstly offers insight into four approaches to using PPPs. Secondly, it formulates 10 recommendations for future action which are broadly applicable to PPPs.

PPPs involve close collaboration between private actors and FIUs and/or law enforcement, with the objective of addressing targeted serious financial crimes such as money laundering and terrorism financing. Legal and ethical frameworks are crucial to the work of PPPs, as they entail the sharing of sensitive personal data on citizens between public and private institutions. PPPs are set up in varying ways, depending on their national legal, political and institutional context. Consequently, no two PPPs operate in precisely the same manner.

The first section of this report therefore consists of a descriptive discussion of four case studies of PPPs, arrived at through document analysis and qualitative research conducted between April 2021 and November 2022. This section provides in-depth insight into PPPs, by describing various aspects such as their legal basis, effectiveness, privacy, proportionality, practices and organisational structure.

This study finds that the variety of PPPs is reflected in the ways in which PPPs address ethical factors. Findings show varying forms and degrees of ensuring legal certainty, and differing practices regarding privacy, oversight, accountability, transparency, and the protection of citizens' rights.

The second section of this report offers ten recommendations. Their aim is to contribute to strengthening PPPs' democratic legitimacy, safeguards, and compatibility with fundamental rights, through a focus on ethics and good governance.

Recommendation 1: Re-evaluate the place of PPPs in the broader AML/CFT architecture.

Recommendation 2: Investigate and mitigate the vulnerabilities of PPPs being used for illegitimate purposes.

Recommendation 3: Align operations with good governance objectives and ethical principles.

Recommendation 4: Establish a solid legal basis prior to the onset of activities.

Recommendation 5: Limit tactical information-sharing to proportionate use.

Recommendation 6: Preserve the privacy and data protection rights of citizens.

Recommendation 7: Enhance transparency of PPPs.

Recommendation 8: Systematically evaluate the impact of PPPs.

Recommendation 9: Task dedicated agencies with oversight of PPPs and ensure that PPPs are held accountable.

Recommendation 10: Ensure that citizens can exercise their rights where they are affected by PPPs.

Stakeholders in PPPs, such as FIUs, private sector actors, policymakers, NPOs, and privacy advocates, are encouraged to implement the recommendations offered in this report, in order to intensify their efforts to bring PPPs into line with fundamental rights, democratic principles and ethical practice, as they continue their efforts in combatting financial crime through public-private partnerships.

List of abbreviations

AML	Anti-Money Laundering
AMLA	Anti-Money Laundering Authority
AMLD	Anti-Money Laundering Directive
AUSTRAC	Australian Transaction Reports and Analysis Centre
BBA	British Bankers' Association
BEIS	Department for Business, Energy & Industrial Strategy
BSOG	Banking Sector Operations Group
Cifas	Credit Industry Fraud Avoidance System
CPS	Crown Prosecution Service
CFT	Countering the Financing of Terrorism
DNB	De Nederlandsche Bank
DPIA	Data Protection Impact Assessment
EFIPPP	Europol Financial Intelligence Public Private Partnership
EU	European Union
Europol	European Union Agency for Law Enforcement Cooperation
FCA	Financial Conduct Authority
FCDO	Foreign, Commonwealth & Development Office
FEC	Financieel Expertise Centrum
FFAUK	Financial Fraud Action UK
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
RCMP	Royal Canadian Mounted Police
FIOD	Fiscale inlichtingen- en opsporingsdienst
FISP	Financial Information-Sharing Partnership
FATF	Financial Action Task Force
FIU-NL	Financial Intelligence Unit Nederland
FSA	Financial Supervisory Authority (Finansinspektionen)
GBP	Great British Pound
GDPR	General Data Protection Regulation
HMRC	Her Majesty's Revenue and Customs
HMT	Her Majesty's Treasury
IISOG	Insurance and Investment Sector Operations Group
JMLIT	Joint Money Laundering Intelligence Task Force
LEA	Law Enforcement Agency
MER	Mutual Evaluation Report
NCA	National Crime Agency
NECC	National Economic Crime Centre
NGO	Non-Governmental Organisation
NL-TFTF	Terrorism Financing Task Force
NOA	National Operations Department
NPO	Non-Profit Organisation
NTFIU	National Terrorist Financial Investigation Unit
OIG	Operational Intelligence Group
OM	Openbaar Ministerie
PCMLTFA	Proceeds of Crime (Money Laundering) and Terrorist Financing Act
PIA	Privacy Impact Assessment

PIPEDA	Personal Information Protection and Electronic Documents Act
PPP	Public-Private Partnership
RFI	Request for Information
SAMLIT	Swedish Anti Money Laundering Intelligence Task Force
SAR	Suspicious Activity Report/Reporting
SEB	Skandinaviska Enskilda Banken
SFO	Serious Fraud Office
SIG	Strategic Intelligence Group
SOU	Statens Offentliga Utredningar
STR	Suspicious Transaction Report(ing)
TF Task Force	Terrorism Financing Task Force
TFTF	Terrorism Financing Task Force
UK	United Kingdom
UKFIU	United Kingdom Financial Intelligence Unit
UNSC	United Nations Security Council
Wwft	Wet ter voorkoming van witwassen en financieren van terrorisme (Anti-Money Laundering and Anti-Terrorist Financing Act)

1. Introduction

This report presents 10 recommendations regarding the ethical and legal challenges of sharing sensitive data between public and private partners through public-private financial information-sharing partnerships[1] in the framework of countering financial crime.

'Public-Private Partnerships' is an umbrella term given to various types of cooperation whereby public and private partners closely collaborate to counter terrorism financing and money laundering through tactical and/or strategic information-sharing.

PPPs are omnipresent in discussions on the future of AML/CFT. They have sprung up in more than 20 countries worldwide in the past years, and their number is steadily growing. Nine EU Member States currently have an operational PPP, and a European EFIPPP has been set up by Europol.[2]

The creation and consolidation of PPPs have been the focus of recent efforts in AML/CFT based on the global standards set by the FATF, the consecutive Anti-Money Laundering Directives that apply within the EU, and national AML/CFT regulations. PPPs are promoted mainly as a means to address the ineffectiveness and inefficiency of the existing efforts to combat money-laundering and the financing of terrorism through transaction monitoring and suspicious activity reporting (SAR) by financial institutions.

There are varying approaches to PPPs within the EU and across the world, based on various legal arrangements and strategic or tactical information-sharing practices.[3]

In July 2021, the EU launched a comprehensive legislative package aimed at strengthening its AML/CFT framework.[4] While in its May 2020 'Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing', the European Commission encouraged the development of public-private partnerships in the fight against terrorist financing and money laundering in the EU,[5] the Roadmap document accompanying the 'Initiative on preventing money laundering and terrorist financing – EU rules on public-private partnerships' acknowledges that PPPs give rise to various challenges impacting fundamental rights and civil liberties, posed by differences in the legal frameworks and practical arrangements of PPPs across the EU Member States.[6]

The challenges posed by PPPs in terms of ethics and fundamental rights remain insufficiently understood. The present research aims to address this gap by offering an analysis of the ethical challenges faced by PPPs.

[1] These public-private financial information-sharing partnerships in the framework of preventing and fighting money laundering and terrorism financing are referred to throughout this report as 'Public-Private Partnerships' or 'PPPs'.
[2] Maxwell, 2020
[3] Maxwell, 2020
[4] Council of the European Union, 2022: p. 4
[5] European Commission, 2020
[6] DG FISMA – Unit D2, 2021

1.1 Study objectives and research questions

This report is the result of a three-year research project on the ethical and legal challenges associated with public-private financial information-sharing, carried out at the University of Amsterdam in the framework of Project CRAAFT.

The general objective of this study has been to contribute to the understanding of the legal and ethical aspects of PPPs aimed at combatting the financing of terrorism. It aims to give insights into existing debates and challenges at both the legal and ethical levels, in order to support policymakers and practitioners in developing PPPs in line with EU fundamental rights and civil liberties. The findings of the study will help policymakers and stakeholders to identify and anticipate ethical and legal challenges associated with PPPs, so they can make informed decisions on the development of PPPs across the EU.

This report builds on the findings of 'Public-Private Financial Information-Sharing Partnerships in the Fight against Terrorism Financing: Mapping the Legal and Ethical Stakes,' a report that was published in January 2021. That report established a framework for approaching and evaluating PPPs in terms of their legal and ethical aspects, based on the academic literature on privacy, proportionality, and the ethics of surveillance.[7]

The first objective of the present report is to gather, analyse, and disseminate information on key practices that PPPs engage in, in relation to five legal and ethical themes identified in the previous phase of this research. These themes are:

- Democratic legitimacy
- Privacy and proportionality
- Mistakes and misuse
- Rights of individuals
- Accountability

In line with this objective, three main research questions have been formulated to guide this study:

- How are PPPs shaped within their national contexts and in relation to the relevant legal frameworks?
- What practices have been developed in PPPs regarding ethical issues, in the context of their institutional, political and legal frameworks?
- What elements of good and bad practice do stakeholders identify regarding the legal and ethical aspects of PPPs?

The second objective of this report is to develop policy recommendations for future action.

1.2 Scope

The geographical scope of section 2 of this report is limited to four selected cases studies. As the 'Mapping the Legal and Ethical Stakes' report indicates, in order to understand the ethical and legal

[7] Dehouck & de Goede, 2021

challenges facing PPPs, one must situate them in the national contexts and in the jurisdictions which shape their institutional forms and practices.[8] Therefore, this report favours an in-depth analysis of a select number of case studies over a broad survey approach. However, the recommendations formulated in section 3 of this report are more broadly applicable beyond the case studies.

The selected case study countries analysed in this report are:

- The Netherlands
- Sweden
- Canada
- The United Kingdom

The case studies were selected with a view to covering PPPs of different types in a range of national contexts and legal environments.

The Dutch Terrorism Financing Task Force was selected for this study because of its continued innovation and relevance in the EU context.

The relevance of the Swedish Anti-Money Laundering Intelligence Task force (SAMLIT) as a case study for this research lies in its position as one of the youngest PPPs of its kind to be established in an EU member state.

The Canadian case was selected as a non-EU, non-tactical information-sharing partnership designed to tackle non-TF threats. It can offer a contrast to findings on EU countries using tactical information-sharing to tackle the threat of terrorism financing.

The relevance of the United Kingdom's Joint Money Laundering Intelligence Task force (JMLIT) as a case study for this research lies in its role as a pioneer and in the fact that it has been recognised by FATF and others as an example of best practice.[9] As the first PPP of its kind, it has served as a model and inspiration for other PPPs around the world.[10]

Throughout the report, there is a focus on counter-terrorst finance, although many aspects can be applicable to anti-financial crime more broadly.

1.3 Methodology

This report is based on a mixed-method approach. Firstly, we conducted desk-based research on PPPs in the four selected case study countries. We reviewed available open sources, including news articles, legislation, parliamentary debates, webinars, and publicly available reporting. Secondly, we conducted a series of semi-structured interviews between April 2021 and November 2022. We interviewed 25 participants, including serving and former members of the selected PPPs, as well as experts in financial crime from the private sector, NGOs, FIUs, policymakers and government representatives. Interviews were held either in person or virtually and were recorded where consent

[8] Dehouck & de Goede, 2021: p. 6.
[9] International Governance & Compliance Association, 2021; FATF, 2018: p. 6
[10] National Crime Agency, sd; Crisp, 2018

was obtained from participants, with the exception of one interview which was held in the form of written questions and answers. Interviews were supplemented with field notes gathered at attended meetings and conferences. Thirdly, we held an expert roundtable to consolidate results and take stock of best practices. Data from the interviews and field notes were coded and analyzed thematically to produce findings and recommendations. In order to ensure confidentiality, interviews are fully anonymized in this report.

An overview of attended field sites can be found in Annex 2.

1.4 Structure of this report

This report is structured around its twofold objective. Section 2 offers a description of the institutional forms, national contexts and key practices of the respective case studies: the Dutch TFTF, the Swedish SAMLIT, the Canadian PPPs, and the UK's JMLIT. Section 3 offers an analysis and synthesis of the study's findings, and proposes recommendations. Lastly, the overall conclusions of the report are presented in section 4.

2. Case studies: findings

This section offers an empirical description of four selected case studies. It details the national context, the institutional form, the legal environment, and key practices of each case study. The objective of this descriptive approach is to offer insight into different approaches to PPPs in relation to the three research questions formulated in the previous section.

2.1 The Netherlands

This section presents the findings about the Terrorism Financing Task force,[11] the Dutch public-private financial information-sharing partnership (PPP) aimed at countering terrorism financing in the Netherlands. It is divided into two broad parts. The first section provides an overview of the Dutch counter-terrorist financing and information-sharing landscape in which the TF Task force operates. The second part describes the TF Task force specifically: its institutional form, its legal basis, its modus operandi and results.

2.1.1 Financial information-sharing in the Netherlands

The Terrorism Financing Task force is part of a wide array of CFT policy instruments aimed at addressing terrorism financing risks, detailed below:

Box 1: CFT instruments in the Netherlands[12]

International legal framework	National legal framework	Other policy instruments
- FATF Recommendations - EU Anti-Money Laundering Directives - United Nations Security Council Resolutions 1267 and 1373 - European Regulation on Controls of Cash Entering or Leaving the EU (Regulation (EC) 1889/2005) - Wire Transfer Regulation 2 (Regulation (EU) 2015/847 on information accompanying transfers of funds	- Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) - Sanctiewet 1977 - Sanctieregeling Terrorisme 2007-II - Wetboek van Strafrecht - Wetboek van Strafvordering - Wet op de inlichtingen- en veiligheidsdiensten 2017 - Tijdelijke wet bestuurlijke maatregelen terrorismebestrijding - Wet op het financieel toezicht - Wet controle op rechtspersonen - Handelsregisterwet 2007 - Fiscale wetgeving - Sociale wetgeving - Wet Bibob - Wet op de economische delicten - Meldrecht Belastingdienst 2003	- National partnerships (TF Task force; CT Infobox; Commissie Meldplicht van Ongebruikelijke Transacties) - International partnerships - Sectoral regulation and conditions - Directives, guidelines and policy plans

[11] Known in Dutch as the 'Terrorismefinanciering Taskforce' or 'TF Taskforce'.
[12] Adapted from van der Veen, Heuts, & Leertouwer, 2019, p. 68

In terms of public-private information-sharing, the AML/CFT framework centres around **transaction monitoring** and SAR by financial institutions, in fulfilment of their legal obligations under the Dutch AML/CFT legislation (Wwft).[13] In 2020, a **private-private** information-sharing partnership was created between five Dutch banks[14] to jointly monitor transactions, called Transactie Monitoring Nederland.[15]

The TF Task force is the Dutch public-private financial information-sharing partnership specifically targeted to terrorism threats. It was created as a **voluntary addition** to the existing regime of transaction monitoring and suspicious transactions reporting as required by law, not as a replacement.[16] It was created with the aim of delivering more targeted, better-quality unusual transactions reports to the FIU.

The TF Task force exists alongside two other **public-private information-sharing partnerships** currently in use in the Netherlands: the Netherlands Serious Crime Task Force and Fintell Alliance Nederland. All three partnerships are directed by the FEC (Financial Expertise Centre), which is the public-private coordinating authority. The Task forces and the Fintell Alliance have different and complementary roles.[17]

The **Serious Crime Task Force** is a public-private partnership which targets money laundering, extreme violence and corruption through brokers and professional money launderers.[18] Its aim is to prevent and detect serious crime and protect the integrity of the financial sector. It consists of four Dutch banks (ABN AMRO Bank, Rabobank, de Volksbank, and ING) on the private side, and the FIOD, FIU-NL, the Public Prosecutor's office[19] and the National Police on the public side.[20]

The **Fintell Alliance Nederland** is an intensive collaboration between the Dutch FIU (FIU-NL) and four Dutch banks: ABN AMRO, Rabobank, de Volksbank and ING.[21] The Fintell Alliance NL is aimed at exchanging knowledge between the FIU and the banks, and to allow obliged entities to receive feedback on their Unusual Transactions Reports. This is meant to strengthen the effectiveness and efficiency of banks' legal obligations to monitor transactions and report unusual transactions. They do this by letting analysts from the banks and FIU work together in a shared physical office. The Fintell Alliance originated in 2018 as a pilot and was established through an 'alliance document' in February 2021. Although it is specifically aimed at the system of transaction monitoring, the Fintell Alliance is also aimed at supporting the two Task forces.[22]

[13] Wet ter Voorkoming van Witwassen en Financieren van Terrorisme (2008), available at https://zoek.officielebekendmakingen.nl/stb-2008-303.html
[14] ABN AMRO, ING, Rabobank, Triodos Bank and de Volksbank. These are the same banks that are part of the TF Taskforce. The partnership was created in 2020. The first joint transaction monitoring has happened in 2021.
[15] Transactie Monitoring Nederland, sd
[16] Mijnheer, 2019
[17] Maxwell, 2020: p. 39-40
[18] Maxwell, 2020: p. 43
[19] 'Openbaar Ministerie'
[20] Convenant Pilot Serious Crime Task Force (2019), available at https://zoek.officielebekendmakingen.nl/stcrt-2019-43629.html
[21] Financial Intelligence Unit - Nederland, 2021
[22] Financial Intelligence Unit - Nederland, 2021; Nederlandse Vereniging van Banken, 2021

Prior to the TF Task force, a comparable project of public-private intelligence exchange had been discontinued by the Ministry for Justice and Security in 2016. In the **discontinued project**, the FIU received names of potential terrorists from the police and forwarded them to banks. The Justice Department and the Dutch privacy supervisor (Autoriteit Persoonsgegevens) had deemed at the time that this was legally allowed. However, later on it appeared to not be legally permitted. The difference between the discontinued project and the TF Task force is that in the latter, the police shares names with financial institutions instead of with the FIU. As explained by the FEC, this difference makes that the TF Task force falls within the confines of the law, based on art. 20 of the 'Wet Politiegegevens' (on which more below).[23]

2.1.2 Terrorism Financing Task Force

The Terrorism Financing Task Force[24] is the Dutch public-private financial information-sharing partnership (PPP) aimed at countering terrorism financing in the Netherlands. Its objective is to protect the integrity of the financial system against threats of terrorism financing, through targeted tactical and strategic information-sharing. The TF Task Force, which was originally established as a pilot in 2017, has matured into a structural collaboration between six private and four public actors.

Establishment

The Terrorism Financing Task Force was set up as a **pilot project in 2017**. The need for a partnership approach arose from a set of **challenges** identified by public and private stakeholders, mainly centred around the **ineffectiveness and inefficiency** of traditional customer due diligence and transaction monitoring.[25]

According to the Dutch Banking Association,[26] the TF Task Force Pilot was created to address the difficulty in properly identifying and filtering transactions with a potential link to terrorism. It claims that the scientific literature shows that there are no waterproof indicators, and that compared to money laundering, terrorism financing is particularly challenging to discover through the transaction monitoring system.[27] It is nearly unfeasible for banks to discover terrorism financing independently, because TF often involves small amounts which are untraceable for banks based on the common indicators. It is more efficient, according to NVB, to search for names provided by the police than to look for a needle in a haystack.[28]

Dutch banks equally expressed the need for more efficiency than the traditional transaction monitoring system is able to deliver. Banks have named **slowness, bureaucracy,** and a system based on distrust as some of the downsides of the transaction monitoring system, and they have voiced the **need for a more targeted approach**, as well as a public-private relationship based on **trust**.[29]

[23] Kouwenhoven, 2018
[24] Known in Dutch as the 'Terrorismefinanciering Taskforce' or 'TF Taskforce'.
[25] Maxwell, 2020, p. 41
[26] Nederlandse Vereniging van Banken (NVB)
[27] Banken.nl, 2018
[28] Kouwenhoven, 2018
[29] Rosenberg & Wester, 2019

In interviews, reference was made to the **substantive terrorist threat level** in the Netherlands, as well as to the emphasis placed on the importance of public-private cooperation in countering the financing of terrorism by both the FATF and the National Coordinator for Counterterrorism and Security (NCTV), as considerations for **legitimizing** the establishment of the PPP. Moreover, the view was expressed that PPPs could help private parties fulfill their aim of making a contribution on the basis of their '**social responsibility**' to help protect the integrity of the sector, while providing **more effectiveness** for public actors.[30]

In 2018, the TF Task Force pilot was evaluated by its partners[31] and extended with one year. The pilot phase of the TF Taskforce was ended in 2019, when the Task Force was established as a **structural activity** in the framework of the Financial Expertise Centre (FEC).[32] The FEC is a partnership between the Financial Markets Authority,[33] the tax authorities, the Dutch Central Bank,[34] FIU-NL, FIOD,[35] the Public Prosecutor's Office, and the Police.[36] It has a supervisory-, control-, investigation- or prosecution-role with the aim of strengthening the integrity of the financial sector.[37]

Composition

The Terrorism Financing Task Force is embedded in the framework of the Financial Expertise Centre (FEC). It initially consisted of five private partners (four banks and one insurance company). In 2020, a fifth bank joined the partnership.[38] It currently consists of the following partners:

Box 2: TF Task Force composition

Private partners	Public partners
- ABN AMRO - ING - Rabobank - De Volksbank - Triodos Bank N.V. - AEGON	- The Dutch National Police - The Public prosecutor's office (OM) - The Dutch Financial Intelligence Unit (FIU-NL) - The Tax Information and Investigation Service (FIOD)

Objectives

Article 2.1 of the 2019 Terrorism Financing Task Force Covenant states the aims of the TF Task Force:

[30] Interview 21, conducted in August 2021
[31] Interview 2, conducted in April 2021
[32] Financieel Expertise Centrum, 2020; FIU-Nederland, 2020: p. 45
[33] Autoriteit Financiële Markten (AFM)
[34] De Nederlandse Bank (DNB)
[35] Fiscale Inlichtingen en Opsporingsdienst (Tax Information and Investigations Service).
[36] FEC, sd
[37] FEC, sd
[38] Financieel Expertise Centrum, 2021

> "To facilitate the collaboration between covenant parties for the purpose of the preventive and criminal combating of terrorism financing, also in the interest of the protection of the integrity of the financial sector."[39]

It is explicitly stated that information may be shared and processed within the legal framework, exclusively for the purpose of identifying, detecting and countering terrorism financing, and as such, making an essential contribution to the fulfilment of one of the tasks of the public parties on one hand, and private parties in their societal role on the other hand.

The FEC states that the activities of the TF Task Force aim to lead to a) mapping the financial networks of those involved in terrorism financing; b) enabling better fulfillment of the gatekeeper function of private parties; c) the availability of better information to the FIU-NL and investigative services to pick up and investigate further.[40]

Legal basis

At its inception as a pilot in 2017, the TF Taskforce was established through a **covenant** called 'Convenant Pilot Samenwerking Bestrijding Terrorismefinanciering', published in the Dutch Government Gazette in July 2017.[41] A second covenant was signed in August 2019, called 'Convenant Terrorismefinanciering Taskforce', which embedded the TF Taskforce structurally.[42]

A covenant is an **informal policy instrument**. It is a signed agreement between parties who are in a horizontal, equal relationship to one another. This form of agreement is **not considered law**.[43]

In a 2022 position paper, the Dutch Banking Association acknowledges that these covenants do **not constitute an adequate legal** basis for Dutch PPPs, arguing that at present, PPPs are:

> "[…] largely dependent on the willingness of all partners to conduct (temporary) pilots and conclude covenants between all partners for a limited period. There is **no adequate legal basis** for the exchange of information between obliged entities, competent authorities and law enforcement, which impedes the functioning of public-private partnerships (PPPs) in the AML/CFT domain."[44]

However, the TF Task Force has operated on the basis of these covenants since 2017. They detail the modalities of cooperation within the partnership on the basis of the existing laws that govern each of the partners.[45]

[39] Art 2.1 Convenant Terrorismefinanciering Taskforce (2019), available at https://zoek.officielebekendmakingen.nl/stcrt-2019-43628.html
[40] Financieel Expertise Centrum, 2020
[41] Convenant Pilot Samenwerking Bestrijding Terrorismefinanciering (2017), available at https://zoek.officielebekendmakingen.nl/stcrt-2017-39920.html
[42] Convenant Terrorismefinanciering Taskforce (2019), available at https://zoek.officielebekendmakingen.nl/stcrt-2019-43628.html
[43] Ministerie van Justitie en Veiligheid, 2020
[44] Nederlandse Vereniging van Banken, 2022: p. 2
[45] Interview 2, conducted in April 2021

The sharing of police information within the TF Task Force is based on art. 20 of the 'Wet Politiegegevens'.[46] This provision specifically allows for the structural sharing of **police information** with third parties through partnerships, under certain conditions and for specific purposes such as maintaining public order or preventing and detecting criminal acts.[47] In the case of the TF Taskforce, this is the invocation of a **'pressing need'** and a **'substantial public interest'** as required by art. 20 of the Wet Politiegegevens, before police information is to be shared with third parties in the context of structural partnerships.[48]

The FEC partners have repeatedly argued for the adoption of a **framework law** on information-sharing through partnerships, in order to significantly strengthen the legal basis of the PPP.[49] This legislation, 'Wet Gegevensverwerking door Samenwerkingsverbanden'[50] has been passed by the Dutch Parliament (Tweede Kamer) on 17 December 2020, and is, at the time of data collection, being considered by the Dutch Senate (Eerste Kamer).[51]

Practices and procedures

The Terrorism Financing Task Force works as a '**Co-location of analysts/Secondment'** model.[52] This means that one or two analysts of each bank spend a number of days per week at a shared physical location. An analyst from the FIU and one from the Police or the FIOD are also present. After coordinating with the Public Prosecutor, the FIOD or the Police shares a concrete 'signal' about a certain subject.[53] The FEC, DNB and NVB are also present at the TF Task Force meetings, but they do not receive any tactical intelligence.[54] Lawyers may have access to act as observers, and the minister and the chief of police may also have access in order to sign off on further-reaching information-sharing, as allowed by the Wet Politiegegevens.[55]

The designated analysts who are part of the so-called **'closed box'**, run the personal data through their respective databases to look at transactions, map networks and determine if there are any suspicious transactions to be found. In case unusual activity is detected, the private partner may report it to the FIU, not back to the TF Task Force.[56] The unusual transaction report which is shared with the FIU, is the only piece of information which is visible to the rest of the compliance department of the relevant bank.[57]

[46] Wesseling & de Goede, 2018: p. 180
[47] Art 20 Wet Politiegegevens (2020), available at https://wetten.overheid.nl/BWBR0022463/2020-01-01
[48] Maxwell, 2020, p. 42; Art 20 Wet Politiegegevens (2020), available at https://wetten.overheid.nl/BWBR0022463/2020-01-01
[49] Wesseling & de Goede, 2018: p. 182
[50] 'Data Processing by Partnerships Act'
[51] Draft legislation: Wet Gegevensverwerking door Samenwerkingsverbanden, available at: https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel%3A35447
[52] Maxwell, 2020: p. 14
[53] Mijnheer, 2019
[54] Wesseling & de Goede, 2018
[55] Rosenberg & Wester, 2019
[56] Openbaar Ministerie, sd
[57] Maxwell, 2020, p. 42; Mijnheer, 2019

Due to the closed box-principle, information exchange is possible without the participating partners having access to each other's systems. Subject **information is shared orally** or temporarily written down on a whiteboard.[58] There is no digital exchange portal.[59]

Private-private information-sharing within the TF Task Force is not possible on a multilateral basis. Bilaterally, information may be exchanged between private partners who are part of the Task Force.[60] Participating financial institutions can compare information with other participating banks insofar as the Wwft allows for it.[61] **Cross-border** information exchange is not directly possible through the TF Task Force, except in the form of international collaboration through the FIU as part of international networks such as FIU.NET and Egmont Group.[62]

Types of information exchanged

Both **tactical and strategic intelligence** are co-developed in the TF Task Force, meaning that typologies, knowledge products, threats and behavioural indicators which do not contain confidential identifying information about subjects or clients are shared, as well as sensitive information and personal data including names of specific individuals, legal entities or other identifying information relevant to a case.[63]

In practice, according to publicly available sources, '**signals**' and the accompanying personal data are shared within the TF Task Force.[64] More specifically, investigative services share, in an early stage, **names** of individuals or legal entities who have been associated with terrorism and terrorism financing, to designated analysts in the banks.[65] The names that are shared are not those of people who are suspected of terrorism, but those about whom the police has an 'indication' that they are involved in terrorism.[66] Besides names, i.e. subject information, '**contextual information**' is also shared.[67]

The two covenants which govern the TF Task Force since 2017 detail the legal bases for the **origins** of the shared information. According to the 2017 and 2019 covenants (art.5), the FIU-NL shares 'relevant information' insofar as it is also processed for its own task. The other public partners share 'police information' insofar as it is also processed for their own tasks. The private partners share 'relevant information' with covenant partners 'based on their own research'. Art. 5 refers to the applicable national legislation and international agreements which govern each of the respective entities, to delineate the information which may be provided by each respective partner.[68]

[58] Interview 23, conducted in October 2022
[59] Wesseling & de Goede, 2018: p. 182
[60] Wesseling & de Goede, 2018: p. 182
[61] FIU-Nederland, 2020: p. 45
[62] Mijnheer, 2019
[63] Maxwell, 2020: p. 13
[64] Wesseling & de Goede, 2018
[65] Openbaar Ministerie, sd
[66] Kouwenhoven, 2018
[67] Maxwell, 2020: p. 40
[68] Art 5 Convenant Pilot Samenwerking Bestrijding Terrorismefinanciering (2017), available at https://zoek.officielebekendmakingen.nl/stcrt-2017-39920.html

Privacy and proportionality

In interviews, the view was expressed that the PPP brought increased respect for privacy as well as proportionality, as an addition to the existing CFT regime.

Regarding **proportionality**, An interviewed participant in the TF Task force expressed the view that

> "The effective combating of terrorism financing is qualified as a **weighty public interest** that requires cooperation between public and private parties and justifies the sharing of information, including Personal Data, with due observance of proportionality within a partnership of public and private parties."[69]

A number of actions were undertaken to limit the **privacy and data protection** impact of the PPP:

Prior to establishment of the TF Task Force Pilot, each partner conducted a **Data Protection Impact Assessment** for its own share in the partnership, and examined its legal capacity to take part in a PPP. Extensive discussion between partners took place, in order to establish a format which allows for information-sharing with respect for the principles of subsidiarity, proportionality and privacy. **The NPO sector** was not consulted or involved in this process,[70] but informal contact with the Dutch Data Protection Authority (DPA) took place during the establishment. According to one interviewee, regular consultation with privacy authorities takes place on an ongoing basis. [71]

With the aim of limiting its **privacy impact**, the TF Task Force operates according to a '**closed box principle**': personal data are not allowed to leave the 'closed box' that is the TF Task Force. They are only shared with bank employees who are part of the TF Task Force. The banks' analysts are not allowed to save the data in the bank's database, nor are they allowed to share the information with colleagues who are not part of the TF Task Force. [72]

All participants in the TF Task Force sign a **non-disclosure agreement** to ensure that information is not shared outside of the TF Task Force, nor with colleagues within their own bank.[73] Moreover, private sector employees participating in the PPP are **screened** by the National Intelligence and Security Service. Breaking the intelligence rules (secrecy) would mean that the person concerned would be excluded from the working group. At the time of data colletion, the data indicated that this had not yet occurred.[74]

There is **no central data processing** within the TFTF. The Covenant Partners in the TFTF independently process the information they obtain within this partnership. This entails that each Covenant Partner is responsible for the proper and **secure storage and retention** of information received in its own systems, in accordance with the **retention periods** applicable to that Covenant

[69] Interview 21, conducted in August 2021
[70] Interview 3, conducted in April 2021
[71] Interview 21, conducted in August 2021
[72] Mijnheer, 2019; Wesseling & de Goede, 2018
[73] Wesseling & de Goede, 2018: p. 182; Interview 21, conducted in August 2021
[74] Interview 21, conducted in August 2021

Partner, using the same security standards as for its own confidential information. Article 6.4 of the Covenant provides that information processed by the Covenant partners for the purposes of the Terrorism Financing Task Force will be kept **no longer than necessary** for the purpose for which the information is provided and to meet legal obligations with which the Covenant partners must comply.[75]

If no SAR is filed, the information received by the Covenant Partner(s) is to be **destroyed** immediately, with due observance of legal obligations.[76]

Transparency

The TF Task Force **does not have a dedicated website**. Its **governance documents, the Covenants, are publicly available.** Publicly available information on the TF Task Force can also be found in press releases, news articles and media interviews, as well as some general information on the websites of participating banks.

Accountability

At the onset, the project leader of the FEC[77] chaired the pilot.[78] At the time of writing, the Public Prosecutor's office (OM) is at the head of the project.[79]

The TF Task Force has a **decentralised structure**, whereby all participating public and private institutions are responsible for their respective part in the endeavour, and participate on their own legal terms.[80] For example, should a **citizen request** information about their personal data being held or processed by the TF Task Force, it is agreed that the request shall be handled not by the Task Force itself or its host institution (the FEC), but by the partner which handles the data.[81]

Interview data indicates that the PPP partners operate in a system of 'mutual accountability' among partners, and that they engage in self-evaluation. The PPP is also under the supervision of the Dutch **Data Protection Authority.**[82]

This suggests a gap in accountability and oversight. If all partners are responsible for their role in the Task Force on their own terms, the question remains who is accountable for the TF Task Force as a whole, in terms of reporting, oversight and the risk of mistakes.

Rights of individuals

Article 7 of the covenants governing the TF Task Force, foresees in the possibility for data subjects to **request information** about their personal data processed in the context of the TF Task Force,

[75] Interview 21, conducted in August 2021
[76] Interview 21, conducted in August 2021
[77] Maarten Rijssenbeek, see Soetenhorst, 2020
[78] Mijnheer, 2019
[79] Financieel Expertise Centrum, 2021
[80] Interview 2, conducted in April 2021
[81] Art 7 Convenant Pilot Samenwerking Bestrijding Terrorismefinanciering (2017), available at https://zoek.officielebekendmakingen.nl/stcrt-2017-39920.html
[82] Interview 21, conducted in August 2021

as well as for rectification and removal of their data. However, as one interviewee stated, although individual subjects are protected by the rights of Sections 2, 3 and 4 of the GDPR, "as long as one of the exceptional grounds of Art. 23 GDPR / Art. 41 UAVG[83] applies, **data subjects will not be informed**."[84]

With regards to **financial exclusion**, no public sources are available which detail debanking practices and procedures in the context of the TF Task Force. In response to questions concerning private partners' responsibilities and obligations regarding financial exclusion of persons identified within the partnership, one interviewee referred to Art. 6.3 of the PPP Convenant, which stipulates that throughout the entire process of processing Information, a principle termed **'GAZO'**[85] applies. According to this principle, wherever possible, Covenant Partners are not allowed to use information obtained within the partnership as a basis for 'interventions', without the approval of the Covenant Partner from whom the information originated.[86]

Effectiveness

An interviewed PPP participant expressed the view that the PPP has **increased efficiency and effectiveness** as an addition to the existing CFT regime. However, they also **declined to disclose** quantitative or qualitative information regarding tactical and strategic information-sharing that has been engaged in by the TF Task Force.[87]

Publicly available, precise data on the impact of the TF Task Force is scarce and fragmented. In the absence of recent public reporting on numbers and cases, little can reliably be said about the effectiveness, privacy impact and proportionality of the TF Task Force, as well as about the risk of bias.

In terms of **absolute data**, publicly available numbers at the time of writing indicate that 8 cases were introduced to the TF Task Force from its inception in June 2017 until December 2017. These cases led to the processing of 133 items of personal data. This shows how a single case or 'signal,' can involve large amounts of personal data through network mapping. In July 2018, it was made public that the Task Force had identified 300 potentially terrorism-related unusual transactions, although no further information is publicly available about these cases.[88] In the same year, it was disclosed in the Dutch media that personal data had been shared with banks in 15 terrorism cases by July 2018. It was not shared on what scale names had been shared during the pilot phase.[89]

Since then, **no recent** absolute numbers have been made public,[90] but some **relative numbers** have been disclosed. In a news article from 2019, the former head of the Pilot claimed that the effectiveness of countering terrorism financing has climbed from 10 to 60 per cent through the TF

[83] Uitvoeringswet Algemene Verordening Gegevensbescherming
[84] Interview 21, conducted in August 2021
[85] GAZO: Geen Actie Zonder Overleg ('no action without consultation')
[86] Interview 21, conducted in August 2021
[87] Interview 21, conducted in August 2021
[88] Wesseling & de Goede, 2018: p. 181
[89] Kouwenhoven, 2018; Banken.nl, 2018
[90] Latest publicly available sources: In an interview on the Dutch Banking Association website of 2019, it was cited that the TF Task Force had generated 300 'useful signals' in 2018 (Nederlandse Vereniging van Banken, 2019); a 2020 RUSI report equally cites the numbers from 2018: approximately 300 reports generated by the TF, in response to 15 cases being briefed to co-located analysts in the first year of the TF Task Force partnership (Maxwell, 2020, p. 42).

Task Force.[91] According to the 2019 Covenant, 6 out of 10 alerts that emerged from the Pilot TF Task Force were useful to the Financial Intelligence Unit, whereas regularly, only 1 in 10 of unusual transactions reports is deemed useful.[92] Lastly, according to Maxwell (2020):

> "Compared to a national average of 10% of standard reporting from regulated entities (i.e. 'unusual' reports) meeting a threshold of FIU-designation as 'suspicious', 64% of NL-TFTF -responsive reporting over a 12-month period met the FIU threshold for suspicion and onward intelligence development and disclosure to law enforcement agencies."[93]

It is known that in its first years of existence, the TF Task Force focused (almost) exclusively on the problem of possible foreign fighters associated with the conflict in Syria and suspected of sympathies with IS.[94] No recent figures are publicly available about the types of TF threats associated with cases processed by the TF Task Force.

2.2 Sweden

This section presents findings about SAMLIT, the Swedish PPP aimed at countering financial crime in Sweden. It is divided into two broad parts. The first section provides an overview of the Swedish AML/CFT and information-sharing landscape in which SAMLIT operates. The second part describes SAMLIT specifically: its institutional form, its legal basis, its modus operandi and results.

2.2.1 Financial information-sharing in Sweden

Since 2014, Sweden has a **national strategy for combatting money laundering and terrorist financing**. The strategy defines goals, priorities and measures necessary in the short and longer term, based on the available knowledge on threats, vulnerabilities and risks. It complements the broader national counter-terrorism strategy.[95]

In recent years, a number of **legislative changes** were made in Sweden aimed at tackling money laundering and terrorism financing, in both administrative and criminal law. The 4th EU AMLD is the point of departure for the implementation of the FATF recommendations in Sweden.[96] It was transposed into Swedish law in 2017.[97]

The primary **legislative cornerstone** of the Swedish AML/CFT system is the 'Act on Measures against Money Laundering and Terrorist Financing' or 'Money Laundering and the Financing of Terrorism (Prevention) Act (2017:630)', covering 22 areas of application.[98]

[91] Mijnheer, 2019
[92] Convenant Terrorismefinanciering Taskforce (2019), available at: https://zoek.officielebekendmakingen.nl/stcrt-2019-43628.html
[93] Maxwell, 2020, p. 42
[94] Wesseling & de Goede, 2018
[95] Ministry of Finance, 2022
[96] Forsman, 2020
[97] Finansdepartementet, 2022
[98] Forsman, 2020

The box below details the **policy instruments** utilised in Sweden to tackle terrorism financing.

Box 3: CFT Policy instruments in Sweden

International legal framework	National legal framework	Other policy instruments
- FATF Recommendations; - United Nations Security Council Resolutions 1267 and 1373 - EU Anti-Money Laundering Directives; - Wire Transfer Regulation 2 (Regulation (EU) 2015/847 on information accompanying transfers of funds; - Directive (EU) 2017/541 on combating terrorism.[99]	- Act (2017:630) on Measures Against Money Laundering and Terrorist Financing;[100] - Ordinance (2009: 92) on measures against money laundering and terrorist financing;[101] - Act (2017: 631) on registration of real principals;[102] - Act (2014: 307) on penalties for money laundering offenses;[103] - Act (2002: 444) on penalties for financing particularly serious crime in certain cases;[104][105] - Proposed: SOU (2021: 42) Strengthened measures against money laundering and terrorist financing.	- National strategy for an effective regime for combatting money laundering and terrorist financing.[106]

The Swedish Police Authority has had a central role in the Swedish anti-financial crime system since 2018. It is the overall responsible entity for coordinating AML/CFT measures, and it is part of SAMLIT and a collaboration with the Swedish FSA.[107]

[99] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA
[100] Lag (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism
[101] Förordning (2009:92) om åtgärder mot penningtvätt och finansiering av terrorism
[102] Lag (2017:631) om registrering av verkliga huvudmän
[103] Lag (2014:307) om straff för penningtvättsbrott
[104] Lag (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall
[105] Finansdepartementet, 2022
[106] Ministry of Finance, 2022
[107] Biggin & Lervik, 2021

The Swedish AML/CFT system has received mixed evaluations. Sweden received a **Mutual Evaluation Report** from the FATF in 2017[108] and a follow-up report in 2018. The country has since been rated compliant on 14 Recommendations, largely compliant on 23 Recommendations, and partially compliant on 3 Recommendations.[109] This leads one author to conclude that Sweden's AML/CFT system is **largely effective**, both on a holistic level and in global comparison. However, the author concedes that despite its positive rating from the FATF, **fundamental flaws** remain in the Swedish AML/CFT system.[110] This is echoed in other evaluations, where unidirectional information flows and limited co-ordination and direction from the centre were identified as fundamental flaws in the Swedish system. Moreover, while awareness is said to be growing among Nordic banks, they are still said to be **lagging behind** their European counterparts.[111]

Financial crime has become a political and cultural issue in Sweden and the Nordics.[112] The issue of combating money laundering and terrorist financing has **featured prominently in the public debate** in Sweden in recent years.[113] In one study, over 40 per cent of respondents rated their country's approach to combating financial crime as 'poor', while less than 20 per cent described systems to deal with such crime as 'very mature'.[114]

Several **AML/CFT scandals** involving SEB, Danske Bank and Swedbank have exposed the banks' vulnerability to be used by criminal networks for money laundering.[115]

Financial information-sharing in Sweden is made possible through the **Swedish Anti-Money Laundering Intelligence Taskforce (SAMLIT)**. SAMLIT was established in 2020. It unites the Swedish Police Authority and the five largest banks in Sweden in a public-private partnership aimed at further strengthening efforts to combat money laundering and terrorist financing.[116]

2.2.2 SAMLIT

Establishment

SAMLIT (Swedish Anti-Money Laundering Intelligence Taskforce) was first established as a **pilot** in June 2020.[117] The project was initiated in 2019 by SEB President and CEO Johan Torgeby, in his role as chairman of the Swedish Bankers' Association.[118] The pilot phase of the project ran until November 2020. The goal of the pilot was to evaluate and **test new methods** for sharing information under the current legislation.[119]

[108] FATF, 2017
[109] FATF, 2018
[110] Forsman, 2020: p. 47
[111] Biggin & Lervik, 2021
[112] Biggin & Lervik, 2021: p. 9
[113] Forsman, 2020
[114] Biggin & Lervik, 2021: p. 9
[115] Van Genugten, 2019; Biggin & Lervik, 2021: p. 9
[116] Swedish Police Authority, 2021
[117] Josefsson & Wrigley, 2021
[118] SEB and banks intensify cooperation with police in fight against money laundering, 2020
[119] Danske Bank, 2020

In early 2021, SAMLIT transformed into a **permanent cooperation** within a formalised framework for cooperation and governance.[120] This includes the promotion of legislative and regulatory changes in order to expand the possibility of information-sharing, and striving towards an increased number of participating banks.[121]

The necessity of a PPP was substantiated by, firstly, a need to **remedy the reputational damage** caused to Nordic banks after the mediatised scandals related to failures in fighting financial crime.[122] Secondly, SAMLIT was created with the aim of addressing the challenges faced by the **shortcomings of the SAR regime**,[123] such as the unilateral flow of information from banks to FIU with little or no feedback, the large number of SAR reports, and a lack of dialogue which made it challenging to address emerging trends and typologies in a timely manner.[124]

As one report found:

> "In 2020, the FIU received 24,500 reports of suspicious transactions. Of these, the organisational operator had stated suspicion of financing of terrorism as the basis for the report in barely 560 cases. […] In order for firms and other relevant actors to be able to discover suspected cases of terrorist financing, they require knowledge of what they need to be looking for. Firms call for more feedback – partly on which type of information the FIU wants, and partly on whether the reports that have been submitted have resulted in further investigation."[125]

The **initiative** for the establishment of SAMLIT was taken by the banks. In the formation process of SAMLIT, **inspiration** was gleaned from the UK's Joint Money Laundering Intelligence Taskforce (JMLIT) and the Dutch Terrorism Financing Task Force (TFTF).[126] Although discussions in the initial formative stages were prompted by consultants, it was decided to not pursue any consultant support in the formation stage of SAMLIT.[127]

Composition

SAMLIT consists of the **five largest banks** of Sweden, along with the Swedish Police Authority, represented by the Intelligence Division at the National Operations Department.[128] One interviewee estimates that in its current composition, around **90% of the Swedish financial flows are covered** by SAMLIT.[129] In the future, SAMLIT is said to strive towards an **increased number** of participating financial institutions.[130]

[120] SEB, sd
[121] Swedbank, 2021
[122] Hoikkala, 2020; Josefsson & Wrigley, 2021; Hoikkala, 2020
[123] Josefsson & Wrigley, 2021
[124] Biggin & Lervik, 2021
[125] The Swedish National Council for Crime Prevention, 2021
[126] Interviews 14 and 15, conducted in April 2022
[127] Interview4, conducted in April 2022
[128] Swedish Police Authority, 2021
[129] Interview 14, conducted in April 2022
[130] Swedbank, 2021

Box 4: SAMLIT composition[131]

Private partners	Public partners
- SEB - Handelsbanken - Nordea - Swedbank - Danske Bank - Swedish Bankers' Association	- The Financial Intelligence Unit at the National Operations Department (NOA)

Legal basis

The SAMLIT pilot project was started fully **within the framework of the existing legislation**.[132] One of the core objectives of the pilot phase was to set up the partnership within the existing legal framework, in order to assess whether that would yield sufficient results or whether legislative changes would be needed.[133] As one interviewee noted, the guiding principle during the formation process was to "keep it simple and do what you can within the limitations of your existing framework."[134]

The legal basis for the exchange of information is substantiated by the obligation for banks to provide, on request from the Swedish Police Authority, all information necessary to investigate money laundering or terrorist financing under the **Money Laundering Act**.[135] The Money Laundering Act only empowers the police authority to request information from banks **bilaterally**.[136]

SAMLIT partners **aim for legislative changes** to facilitate and expand the work of SAMLIT.[137] Within the current confines of the law, participating banks in SAMLIT are allowed to collectively share information on methods, suspicious transaction patterns and new types of crime that have been jointly identified.[138] SAMLIT aims to promote legislative changes to expand the possibilities of information-sharing.[139] These changes would focus mainly on **bank secrecy**, in order to render it possible to share relevant information between participating financial institutions.[140] Specifically, interviewed stakeholders expressed the intention to expand the legal basis of SAMLIT to allow for the **exchange of tactical information multilaterally**.[141]

131 SEB, sd
132 SEB and banks intensify cooperation with police in fight against money laundering, 2020
133 Interview 14, conducted in April 2022
134 Interview 14, conducted in April 2022
135 Swedish Police Authority, 2021
136 Danske Bank, 2020
137 SEB and banks intensify cooperation with police in fight against money laundering, 2020
138 Danske Bank, 2020
139 Swedbank, 2021; Hoikkala, 2020; Menou, 2021a
140 Swedish Police Authority, 2021: p. 18-19
141 Interviews 15, 16 and 17, conducted in April 2022

Objectives

The primary objectives of SAMLIT have been adopted verbatim from the objectives of JMLIT, centring around the keywords to '**detect, protect and disrupt**'.[142]

Mainly, the objective of SAMLIT is to improve the ability to identify money laundering and terrorism financing, in order to **secure evidence** for the prosecution of individuals and companies.[143]

The objective is not only retrospective (aimed at prosecution), but also **preemptive**, i.e., preventing terrorist attacks, shootings and explosions, as well as detecting and disrupting crimes at an earlier stage, or preventing them from ever being committed.[144]

Interview data indicates that SAMLIT **focuses mainly on money laundering** rather than terrorism financing, due to a focus in police efforts on tackling organised crime in Sweden.[145] Specifically, gang crime was identified as one of the priorities for SAMLIT, as Sweden has been increasingly plagued by gang-related shootings, bombings and grenade attacks.[146] **Data on the ratio** of money laundering-related cases versus terrorism financing cases processed through SAMLIT, is confidential and **could not be disclosed** by interviewees.[147]

Future directions for SAMLIT which were identified in interviews, include its establishment as a **legal entity**, the integration of **more financial institutions**, the development of **KPIs to measure its outputs**, and the expected **legislative changes** to allow for **private-private information-sharing**, which would lead to **technological developments** within SAMLIT through the integration of Privacy Enhancing Technologies.[148]

Types of information exchanged

SAMLIT engages in **both tactical and strategic-level** information-sharing.[149]

Strategic-level information-sharing happens as part of the **Strategic Intelligence Group (SIG)**, which is currently a **pilot**.[150] At this level, SAMLIT partners engage in exchanging information regarding new approaches, types of crimes and patterns that have been jointly identified.[151] The objective of the Strategic Intelligence Group is to **mitigate the impact of the limits to bank-to-bank sharing** of tactical information, posed by Swedish law, by sharing **themes, patterns and trends at an aggregate level.** This includes types of persons, modus operandi, methodologies, emerging financial crime threats and issues, at an **anonymised** level. In the first instance, this information is used to improve policy and controls within the internal frameworks of each bank. Secondly, this information can be used to identify legal loopholes that are exploited for financial

[142] Maxwell, 2020: p. 38
[143] SEB, sd
[144] Swedbank, 2021; SEB and banks intensify cooperation with police in fight against money laundering, 2020
[145] Interview 14, conducted in April 2022
[146] Milne, 2021
[147] Interview 15, conducted in April 2022
[148] Interview 18, conducted in April 2022
[149] Maxwell, 2020, p. 38
[150] Interview 14, conducted in April 2022
[151] Swedbank, 2021

crime and to lobby for legislative changes, improvements to enforcement, or judicial prosecutions.[152]

At the tactical level, SAMLIT partners **share tactical intelligence bilaterally** from the FIU to the banks. This information can include names of persons or companies, contextual information about cases, and other information that is deemed necessary. This **contextual information** may include relations between companies and persons of interest, company locations and information on '**socially vulnerable areas**',[153][154]

As SAMLIT develops, it aims for legislative and regulatory amendments to allow for banks to more freely engage in **private-private sharing** of confidential (tactical) information.[155]

Practices and procedures

The operations of SAMLIT are laid down in the following **governance documents**, which contain the governance agreements and terms of reference. They are internal documents and are **not publicly available**.[156]

- A formal Governance Charter,[157] detailing the purpose of each committee, roles and mandates, staffing and experience;[158]
- Standard Operating Procedures, approved by all relevant members,[159] which outline the procedures for Requests For Information;[160]
- Steering documents, which have been signed and advised on by the legal department of each bank;[161]
- Terms of Reference for the working groups.

The image below provides an overview of how SAMLIT is **structured**.[162]

[152] Interview 18, conducted in April 2022
[153] Defined by the interviewee as 'socio-economic areas with high crime rates.'
[154] Interview 15, conducted in April 2022
[155] Josefsson & Wrigley, 2021
[156] Interview 18, conducted in April 2022
[157] Maxwell, 2020: p. 38
[158] Interview 15, conducted in April 2022
[159] Maxwell, 2020: p. 38
[160] Interview 15, conducted in April 2022
[161] Interview 15, conducted in April 2022
[162] Image source: Swedish FIU

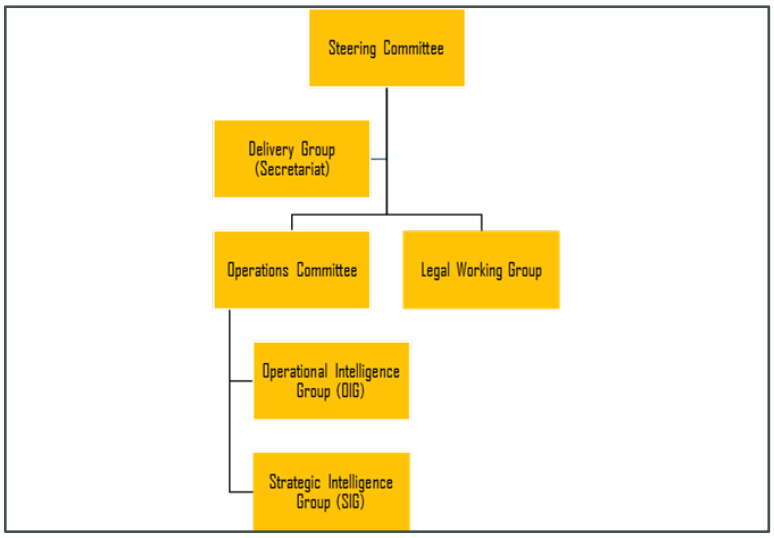

Image 2: SAMLIT structure. Source: Swedish FIU

The **Steering Committee** is responsible for the overall oversight of SAMLIT. Dedicated management and secretariat support exist for Operations and Steering Committees.[163]

The **Strategic Intelligence Group** is a pilot project dedicated to sharing strategic information such as typologies and threats.[164]

The **Legal Working Group** fulfils multiple functions within SAMLIT. Firstly, it examined the **boundaries and consequences** of SAMLIT operations at its formation stage. It advised on the limits to private-private information-sharing between participating banks, resulting in the two-step process for sharing tactical information, detailed below.[165] Secondly, it is involved in examining **lobby efforts on legislative changes** needed to increase effectiveness for SAMLIT.[166] Thirdly, it advises on the **proportionality test** applied by the FIU to RFI's, i.e. determining the threshold of the minimum necessary information to be shared with banks.[167]

In the **Operational Intelligence Group (OIG)**, specialist vetted financial crime investigators of each participating bank meet regularly to receive tactical intelligence from the FIU.[168] During these meetings, the police provides an update on ongoing **investigations** and/or introduces new investigations. Following those meetings, specific requests are filed to the banks through the GoAML system.[169]

The **frequency** of OIG meetings is approximately every 2-3 weeks.[170] Around 10 persons are present in OIG meetings, i.e., one or two persons from each bank and one or two persons from the FIU.[171] They are held at the FIU headquarters at the National Operations Department

[163] Maxwell, 2020: p. 38
[164] Interview 14, conducted in April 2022
[165] Interview 18, conducted in April 2022
[166] Interview 14, conducted in April 2022
[167] Interviews 14 and 15, conducted in April 2022
[168] Swedbank, 2021
[169] Interview 18, conducted in April 2022
[170] Interview 18, conducted in April 2022
[171] Interview 15, conducted in April 2022

(NOA).[172] At the time of data collection, the majority of SAMLIT meetings had been held **remotely due to the Covid-19 restrictions** which had been in force since the establishment of SAMLIT.[173]

The practices of SAMLIT were developed while taking into account that Swedish bank secrecy laws prevent banks from sharing the received tactical intelligence with each other.[174] As a result, information-sharing happens **both through a software platform and in a physically co-located space**. Only general information concerning the investigation is shared as part of the OIG meetings, while the names of individuals or companies are shared bilaterally via the GoAML system.[175]

With the aim of complying with the legal restrictions on bank-to-bank information-sharing, tactical information-sharing in the OIG follows a **two-step procedure**. In an initial OIG meeting between bank officials and the FIU, OIG briefings are anonymised. The police provide a description to the vetted bank representatives containing the **content of the investigation**, what they are trying to target, what their focus points are, and how the banks might try to look for it within their information, without naming individuals. In the second step, the banks receive formal, non-anonymised requests for information via the **GoAML platform bilaterally**, containing the names of individuals and companies of interest.[176]

As one interviewee explained, tactical information-sharing follows an **iterative process** that can be likened to a **funnel.** In the initial stages of an investigation, a broad range of key subjects of interest will be shared. Based on the SARs filed following the initial round of requests for information, some individuals or companies may be deemed to no longer be of interest, while others may be added.[177] Once individuals are cleared of suspicion, the banks are not allowed to retain the information concerning the individual.[178]

The exposure may initially concern only one bank, but may be expanded to include other participating banks, based on the feedback on subjects' transaction activity. The end of the iterative cycle is reached when the police deems that it has received sufficient information on

> "who this person is, how they've transacted, and the connections that they've got, that we no longer need information."[179]

At the same time, a **reversed funnel-effect** was also observed by one interviewee, who mentioned a **'multiplier effect'** as a result of Requests for Information (RFI):

[172] SEB and banks intensify cooperation with police in fight against money laundering, 2020
[173] Interview 18, conducted in April 2022
[174] Swedish Police Authority, 2021: p. 17
[175] Interview 15, conducted in April 2022
[176] Interview 18, conducted in April 2022
[177] Interview 18, conducted in April 2022
[178] Interview 14, conducted in April 2022
[179] Interview 18, conducted in April 2022

> "Every time that we have a new case presented by the police, there is a significant multiplier of what we identify inside the banks and can then feed back to the police."

Based on the requests made by the police, the banks map broader transaction flows to identify how money is circulating,

> "So you are able to identify a bigger picture than the one that was served up by the police."[180]

SAMLIT operates as a **relatively low-tech** cooperation.[181] SAMLIT is not intended to serve as a replacement, but as a complement to the regular SAR regime. Therefore, the same systems were used which were already in use to comply with Suspicious Activity Reporting, i.e., GoAML.[182] According to some interviewees, there is room for improvement in terms of SAMLIT's use of technology, in particular with regards to Privacy Enhancing Technologies. Interviewees expected technological advancements to be prioritised following expected future developments in terms of private-private information-sharing based on the proposed legislative changes.[183]

The operational process regarding **offboarding clients** follows the procedures put into place as part of the regular SAR process. In practice, this means that any customer alert raised as a result of a request for information through SAMLIT, is processed as if it was a transaction monitoring alert.[184] According to one interviewee, in some instances, the police may request the bank to hold off on offboarding when they are planning a larger arrest of several persons.[185] However, this was contradicted by another interviewee, who stated that the FIU does not advise on offboarding matters.[186]

Unintended consequences

When asked about unintended consequences of SAMLIT operations, the main unintended consequence identified by a senior official involved in SAMLIT, was the potential for the **displacement of money laundering and terrorism financing activities** to financial institutions not involved in SAMLIT, or to other avenues where it can escape from scrutiny. The interviewee deemed that unintended consequences do not pose an additional risk of occurring as part of SAMLIT operations, as it operates within the same legal framework as the SARs regime. As the interviewee explained:

> "As of now, we're doing everything within the tools and the legislation that we have already in place. So, we're not increasing the risk anywhere."

[180] Interview 14, conducted in April 2022
[181] Interview 16, conducted in April 2022
[182] Menou, 2021b
[183] Interview 16, conducted in April 2022
[184] Interview 18, conducted in April 2022
[185] Interview 14, conducted in April 2022
[186] Interview 15, conducted in April 2022

The interviewee added that if SAMLIT were to evolve towards a system where a shared database containing sensitive data would be used to share information between banks, challenges could arise which should be analysed and understood.[187]

A theme that emerged from interviews which requires further analysis with regards to the potential for **profiling and bias**, is the mention of 'vulnerable areas' which are under particular scrutiny with regards to (financial) crime, and which are an area of focus for SAMLIT according to interview data.[188] This term refers to the practice by the Swedish Police to **designate certain geographic areas as 'crime-exposed areas'**, in which citizens' exposure to crime has a strong impact on their daily lives in the local community. According to Guldaker et al. (2021), the mapping and designation of those areas is based on the subjective experiences and perceptions of police officers.[189]

Privacy and proportionality

Sweden's **strict privacy laws** are a point of contention concerning the work of SAMLIT. When setting up the partnership, questions were raised regarding the compatibility of JMLIT-like operations with Sweden's privacy framework.[190]

The main point of contention at the moment is the **relaxing of bank secrecy laws**, which is a recurring request by the banking sector. This would allow for information-sharing between participating banks.[191] In interviews, SAMLIT partners repeated the need for banking secrecy laws to be relaxed to allow for this multilateral private-private information-sharing. The Swedish bankers' association has also expressed this opinion publicly in the past.[192]

Interview data indicates that **no Privacy Impact Assessment** has been conducted on SAMLIT.[193]

A **proportionality test** is applied to RFIs by the FIU. Prior to filing an information request with the banks, an internal meeting is convened within the FIU to determine the content of the request for information. A legal advisor conducts a proportionality test to determine whether no more information will be shared than is strictly necessary for the purposes of the investigation.[194] Bank representatives do not receive any information regarding the phase prior to the RFI, i.e. on the source of the intelligence. Banks are obliged by law to provide information following a request, meaning that they have no capacity to refuse, as this would lead to sanctions.[195] However, they do have a possibility to challenge the quality of the information request. In the formation phase of SAMLIT, banks have also been consulted on what types of information should be contained in the content of RFIs.[196]

[187] Interview 14, conducted in April 2022
[188] Interviews 14 and 17, conducted in April 2022
[189] Guldåker, Hallin, Nilvall, & Gerell, 2021
[190] O'Neill, 2019
[191] Forsman, 2020: p. 47
[192] Swedish Bankers' Association, 2019
[193] Interview 15, conducted in April 2022
[194] Interview 15, conducted in April 2022
[195] Interviews 14, 15 and 17, conducted in April 2022
[196] Interview 18, conducted in April 2022

Transparency

SAMLIT **does not have a dedicated website**, nor does it publish its **governance documents or terms of reference** publicly.[197] Publicly available information on SAMLIT can be found in press releases, news articles and media interviews, as well as some general information on the websites of participating banks and the Swedish government. Transparency International Sweden mentioned the **lack of transparency** as a point of improvement as SAMLIT evolves from the pilot stage into a more formal cooperation. It noted that a dedicated website, information made available, and a formal point of contact for SAMLIT such as a general email address, should be minimum requirements in terms of transparency.[198]

When asked about transparency, the following explanations were gleaned from interviews: Firstly, when asked about the reason for governance documents and terms of reference not being publicly available, one interviewed bank official's response was that SAMLIT does not publish its governance documents because it considers its operational capability to still be at a **developmental stage** where it does not have a sufficient level of maturity to offer this type of transparency.[199] This stance was reiterated by other interviewees, stating that transparency is not at the top of the agenda at this stage. The interviewees stated that its priority is to demonstrate results before offering more transparency.[200] However, interviewees stressed that this does not mean that SAMLIT operations are kept secret.[201]

Secondly, one interviewed bank official stated that since SAMLIT is a voluntary collaboration which is funded by the participating banks, it **does not have a democratic imperative** to be transparent in its documentation at this point in time. The interviewee added that this may change in the future, if SAMLIT were to become a legal entity or start receiving public funds.[202]

Accountability

At the time of data collection, the partnership was chaired by Martin Johansson, Senior Advisor to the CEO of SEB. In the future, the objective is to create a **rotating chairmanship** between the different banks. The chairman of SAMLIT does not have insight in the content of the cases that are subject to information requests as part of SAMLIT.[203]

No external body is charged with oversight of SAMLIT. There is no parliamentary discussion on the evaluation of SAMLIT, nor does a **privacy authority** keep oversight of SAMLIT operations.[204]

According to interviews, security concerns were one of the key discussion points with regards to setting up the terms of reference and governance procedures of SAMLIT. Bank employees

[197] Interview 15, conducted in April 2022
[198] Interview 19, conducted in May 2022
[199] Interview 18, conducted in April 2022
[200] Interviews 15 and 16, conducted in April 2022
[201] Interview 15, conducted in April 2022
[202] Interview 18, conducted in April 2022
[203] Interview 14, conducted in April 2022
[204] Interview 14, conducted in April 2022

participating in the OIG undergo high-level national **security vetting**, suitable for the receipt, dissemination and management of sensitive information.[205]

Sweden has multiple **watchdogs** that act as safeguards against misuse and abuse, such as the Justice Chancellor and the Ombudsman, who serves as a point of contact for citizens who believe rights have been violated or risk being violated. Civil society, including Transparency International Sweden, also considers itself to be in a position to raise alarms publicly if they had reason to believe that harms to fundamental rights, abuses or mistakes would occur as a result of SAMLIT operations.[206]

Interviewees also mentioned the existence of **whistle-blower protection programmes** in Sweden, which act as an incentive for SAMLIT participants to speak out in case of misuse or abuse.[207]

Effectiveness

According to interviews, information has been shared within SAMLIT in the context of **between 13 and 17 investigations** since its inception.[208] The interviewed banking officials did not have information on the numbers of requests into specific individuals or companies that had been made to banks in the context of those investigations, other than the estimate that banks receive a request from the FIU approximately every three weeks. The number of requests varies from bank to bank, since not every bank is involved in every investigation, and the content of requests made to banks in the context of one investigation, may also vary.[209]

The **impact** of SAMLIT has **not been measured** in a quantifiable way to date. One of the reasons identified was that convictions based on SAMLIT operations may take many years, while SAMLIT is still in its beginning phases.[210]

No cost-effectiveness study has been done on SAMLIT, due to the early stages of its development. One of SAMLIT's objectives for the future is to establish a set of metrics to enable the identification of SAMLIT's efficacy, compared to its costs in terms of personnel allocation.[211]

At the time of data collection, SAMLIT partners were working on **developing KPIs** to measure the impact of SAMLIT more systematically. These indicators revolve around raising knowledge, long-term results, and formal investigations.[212]

SAMLIT partners have publicly expressed generally positive evaluations of SAMLIT. According to the 2020 annual report of the Swedish FIU:

> "SAMLIT has (…) resulted in banks taking measures directed at the individuals in question and improving their monitoring of modus

[205] Interviews 15 and 18, conducted in April 2022
[206] Interview 19, conducted in May 2022
[207] Interview 16, conducted in April 2022
[208] Interviews 15 and 18, conducted in April 2022
[209] Interview 18, conducted in April 2022
[210] Interview 14, conducted in April 2022
[211] Interview 18, conducted in April 2022
[212] Interview 15, conducted in April 2022

> operandi. Early on, it was apparent that the project produced results and the investigations have grown. Money was seized, preliminary investigations were initiated and parallel cases opened."[213]

CEO of SEB Johan Torgeby was also quoted saying that SAMLIT seems to be much more effective than the traditional compliance regulation.[214]

In addition, the following impacts of SAMLIT were identified by interviewees: it provides the police with the ability to effectively capture and review information on an entire network **simultaneously**, improving the speed and quality of the output, as well as evidence collection;[215] the **improvement of SARs** through better feedback loops;[216] the establishment of **trust relationships and a better understanding** between public and private entities.[217]

SAMLIT was received as **a welcome development** by Transparency International Sweden, which considers it to have potential in terms of more efficient allocation of resources and more effectiveness in the fight against ML and TF in Sweden, particularly in light of the shortcomings that have been observed in recent years.[218]

2.3 Canada

This section presents findings about the Canadian PPPs aimed at countering financial crime. It provides an overview of the Canadian information-sharing context, followed by a description of the institutional form, legal basis, modus operandi and impact of Canadian PPPs aimed at tackling financial crime.

2.3.1 Financial information-sharing in Canada

In Canada, public-private partnerships focus on the financial component of specific types of criminal activity, as opposed to money laundering or terrorism financing more broadly.[219] A distinction is made between public-private 'awareness'-based partnerships and targeted projects.

Awareness projects use research and indicator-creation to enhance reporting on predicate offences. They have a dual purpose of heightening general awareness amongst relevant groups (e.g. regulatory, anti-money laundering professionals, etc.) and enhancing STRs filed to FINTRAC on potential money laundering related to a specific predicate offence.[220]

There are six public-private awareness partnerships: **Project Protect**, set up in 2016, was the first public-private partnership launched with the aim of combating human trafficking in the sex

[213] Swedish Police Authority, 2021: p. 17
[214] Milne, 2021
[215] Interview 19, conducted in May 2022
[216] Interviews 14 and 19, conducted in April and May 2022
[217] Interviews 15 and 16, conducted in April 2022
[218] Interview 19, conducted in May 2022
[219] Interview 6, conducted in August 2021
[220] Maxwell, 2020

trade;[221] **Project Guardian**, targeting money laundering associated with fentanyl trafficking, launched in 2018; **Project Chameleon**, the public-private partnership tackling romance fraud since 2017; **Project Athena**, launched in 2019 with the aim of combating money laundering in British Columbia and across Canada;[222] **Project Shadow**, combating money laundering associated with online child exploitation; **Project Organ**, launched in 2017 with the objective of targeting organ trafficking or trafficking of persons for the purpose of organ removal.[223]

Targeted investigations address a specific criminal offence suspected of being perpetrated. They comprise various forms of interaction between the public and private sectors, such as FINTRAC's proactive disclosure of STRs to law enforcement agencies, the issuance of court orders by law enforcement to private sector entities to obtain information directly, or briefings from law enforcement agencies to banks on certain disclosable pieces of information pertaining to open investigations. Targeted projects have been set up i.a. to address drug trafficking, fraud and illegal gambling.[224]

Canada does not have a financial information-sharing partnership which specifically tackles **terrorism financing.** FINTRAC issues guidance to reporting entities on indicators of terrorism financing, but they are not in the context of a PPP.[225]

2.3.2 Canadian PPPs

Establishment

Aside from the legal basis, three key factors for the establishment of PPPs in Canada were identified during interviews. Firstly, the existence of sufficiently strong **trust relationships** between all parties involved, largely relying on interpersonal relationships forged through long-standing working relationships and staff turnover between the prospective partners. Secondly, the willingness of one of the major Canadian financial institutions to **take the lead** in the partnership. Thirdly, the presence of a **pressing need** (public interest-test) concerning the specific type of financial crime the PPP is aimed at targeting, as a way of ensuring the legitimacy and public buy-in of the PPP.[226]

Interviews indicated that at the time of data collection, the latter two conditions had not been sufficiently fulfilled to lead to the creation of a PPP specifically tackling **terrorism financing**.[227]

Box 5: Establishment of Project Protect

In 2016, human trafficking survivor Timea Nagy addressed the audience at an ACAMS conference in Toronto. After making a compelling account of her experience as a human trafficking survivor, she challenged the audience to intensify their efforts against human trafficking. The audience consisted of financial institutions, the FIU community and

[221] Bradshaw, 2020
[222] FINTRAC, 2020
[223] Maxwell, 2020
[224] Maxwell, 2020
[225] See: Special Bulletin on Ideologically Motivated Violent Extremism (July 2021), available at https://www.fintrac-canafe.gc.ca/intel/bulletins/imve-eng
[226] Interview 6, conducted in August 2021
[227] Interview 6, conducted in August 2021

representatives of law enforcement. An audience member from Bank of Montreal responded by initiating to take up the lead of what would become Project Protect, the Canadian public-private financial information-sharing partnership tackling human trafficking. FINTRAC, law enforcement and financial institutions agreed that within the existing system under the PCMLTFA, a more targeted effort could be made to address the specific societal issue of human trafficking in the form of a PPP.[228]

Composition

The composition of the partners who participate in the Canadian public–private partnerships varies according to the underlying predicate offence that is being addressed, although major reporting entities such as banks, the federal police (RCMP) and the national FIU (FINTRAC) are foundational partners for all awareness projects.[229]

Canadian PPPs include participation from **non-profit organisations**. Project Protect includes NPOs that provide frontline services to survivors of human trafficking.[230] They are consulted to provide input on the analytical basis of indicators and to identify potential **unintended consequences** of indicators.[231] The Canadian Anti-Fraud Centre participates in Project Chameleon,[232] while the Canadian Centre for Child Protection is a lead partner in Project Shadow.[233]

Legal basis

Canadian PPPs are established **within the existing legal framework,** in relation to clearly defined predicate offences. Due to the form the PPPs take, no legislative changes were required for their creation.[234] They operate within the framework of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act[235] (**PCMLTFA**),[236] which establishes reporting entities' obligations in combating the laundering of proceeds of crime and the financing of terrorist activities in Canada, as well as the creation of the Canadian FIU, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).[237]

The Canadian Charter of Rights and Freedoms prescribes the **limitations** on what information reporting entities, FINTRAC and law enforcement partners are allowed to collect and share under the PCMLTFA.[238]

[228] Interview 6, conducted in August 2021; Mari, 2017
[229] Maxwell, 2020
[230] Maxwell, 2020
[231] Interview 6, conducted in August 2021
[232] Maxwell, 2020
[233] Bradshaw, 2020
[234] Interview 6, conducted in August 2021
[235] The PCMLTFA was created in 2001 as an amendment to The *Proceeds of Crime (Money Laundering) Act* (FINTRAC, sd)
[236] Proceeds of Crime (Money Laundering) and Terrorist Financing Act (S.C. 2000, c. 17)
[237] FINTRAC, sd
[238] Interview 6, conducted in August 2021

Types of information exchanged

Canadian public-private partnerships are limited to sharing **strategic intelligence**, meaning that typologies, macro-trends, threats and behavioural indicators can be co-developed and shared within the partnerships. Strategic information does not contain personally identifying information about subjects or clients.[239]

No tactical information, i.e. sensitive information and personal data including names of specific individuals, legal entities or other identifying information relevant to a case[240] is shared as part of the partnerships, as **no legal basis** was found that would permit reversing the flow of information to proactively share tactical intelligence such as information on named potential subjects with private partners within PPPs. **Judicial authorisation** is required for this type of information request to be issued by law enforcement, as part of criminal investigations on an ad hoc basis.[241]

Practices and procedures

As Canadian PPPs are limited to strategic information-sharing whereby the flow of information is not reversed, PPPs are largely governed according the procedures under the PCMLTFA predating the PPP model.[242]

Information within Canadian PPPs flows as follows: FINTRAC creates **Operational Alerts** containing **strategic guidance** for reporting entities on the types of indicators and red flags they should be looking for, with the aim of improving the quality of suspicious transaction reporting.[243] Reporting entities can use this information to file **suspicious transaction reports (STRs)** to FINTRAC, which is mandated to disclose this information from their database to law enforcement, if it finds that the legal thresholds are met.[244] Law enforcement, in turn, can utilise the received intelligence towards prosecution.[245]

The **reversed flow of information** consists of a written **feedback** mechanism whereby law enforcement informs FINTRAC of the usefulness of disclosed information. This feedback cannot directly be passed on to reporting entities. It is stripped of all identifying case information to inform the **strategic-level guidance** that FINTRAC provides to reporting entities. Only a very limited degree of generalised positive feedback can be given by the FIU to reporting entities when law enforcement investigations have obtained successful results due to the information generated by their STRs. This feedback may contain no information on specific cases or STRs, as FINTRAC is obliged to act as a passive recipient of reporting entities' information, and to be watchful for the risk of tipping off.[246]

As mentioned, no tactical information requests to reporting entities can be made in the Canadian PPP model. In order to reverse the flow of information at the tactical level, the information

[239] Maxwell, 2020
[240] Maxwell, 2020
[241] Interview 6, conducted in August 2021
[242] Interview 6, conducted in August 2021
[243] Interview 6, conducted in August 2021
[244] Interview 6, conducted in August 2021
[245] Mari, 2017
[246] Interview 6, conducted in August 2021

obtained through STRs and passed on to law enforcement by the FIU may be used as grounds for law enforcement to obtain **judicial authorisation** to request information of reporting entities in particular cases.[247]

Rights of individuals

A study on **de-risking and financial exclusion** in the Canadian context was published by Amicelle & Iafolla in 2018,[248] but at the time of data collection, there was no information available about de-risking practices relating specifically to PPPs. Notably, as an extension of Project Shadow, Scotiabank partnered with Canadian NGOs to launch the 'Financial Access Program', aimed at ensuring financial access and limiting **financial exclusion** of human trafficking survivors. It links survivors of human trafficking to financial institutions in order to renew their access to the financial system, and developed a trauma-sensitive approach to customer onboarding, as well as financial literacy programs.[249]

In principle, the Personal Information Protection and Electronic Documents Act (PIPEDA) provides Canadians who wish to be informed of disclosures made to FINTRAC, with a procedure to file an **access request**. However, PIPEDA provides for exceptions in cases of money laundering and terrorism financing, that allow FINTRAC to object to information requests if it is of the opinion that compliance with the request could reasonably be expected to be injurious to the detection, prevention or deterrence of ML/TF. Section 7 of PIPEDA also suspends the knowledge or consent-principle for circumstances that relate to ML/TF.[250]

Accountability

Each partnership is headed by one of Canada's major financial institutions. The **leading partner** of Canadian partnerships is a fixed role that is taken up voluntarily by a financial institution.[251]

FINTRAC is mandated to ensure that the data under its control is protected in light of Canada's privacy laws.[252] FINTRAC undergoes biennial audits by the **Office of the Privacy Commissioner** on the measures it takes to safeguard the personal information that it receives and collects.[253] In 2009 and 2013, these audits found that FINTRAC collects and stores too much information. The Privacy Commissioner urged FINTRAC to limit the amount of personal information it accepts and holds.[254]

Effectiveness

Interviews revealed that PPP partners experience **difficulties in measuring** the effectiveness of strategic PPPs in precise data.

[247] Interview 6, conducted in August 2021
[248] Amicelle & Iafolla, 2018
[249] Canada NewsWire, 2021; Market News Publishing, 2021
[250] Office of the Privacy Commissioner of Canada, 2012
[251] Interview 6, conducted in August 2021
[252] Interview 6, conducted in August 2021
[253] FINTRAC, 2020
[254] Pilieci, 2013; Prince George Citizen, 2009

According to interviewees, the **main metrics** used to gauge the effectiveness of Canadian PPPs are the following: firstly, a written feedback mechanism from law enforcement agencies to FINTRAC on the usefulness of disclosed intelligence.[255] Secondly, the quantity of STRs filed by reporting entities, whereby an increase in STRs following the establishment of a PPP indicates its effectiveness. Thirdly, FINTRAC keeps track of media mentions on successful investigations into the predicate offenses regarding which they have a PPP, as a measure of effectiveness. Counting charges of money laundering specifically, was indicated to be a less useful practice to measure effectiveness in the Canadian context.[256]

Canadian PPPs regularly offer **transparency** on the results and impact of their activities:

In its annual report, FINTRAC disclosed that it received thousands of suspicious transaction reports relating to the trafficking of illicit fentanyl in 2019–20 as a result of **Project Guardian**. With this information, FINTRAC generated 134 disclosures of actionable financial intelligence in support of the money laundering and fentanyl/drug trafficking investigations of Canada's municipal, provincial and federal police agencies.[257]

In 2019-20, FINTRAC provided 251 disclosures of financial intelligence to Canada's police forces in relation to **Project Protect**.[258] By the end of 2020, it was reported in the Canadian press that Project Protect had yielded a 750 per cent increase in STR-reporting, leading to more than 500 disclosures by FINTRAC to law enforcement agencies, and resulting in the rescue of more than 100 victims of human trafficking.[259] In July 2021, FINTRAC reported that 979 packets of intelligence had been disclosed to police and law enforcement agencies in the 5 years prior, as part of Project Protect.[260]

In 2020, 52 disclosures were reported to be made by FINTRAC to law enforcement agencies in relation to **Project Athena**, and 74 disclosures in relation to **Project Chameleon**.[261]

From autumn 2019 to mid-2020, 20 disclosures were reported in relation to **Project Shadow**.[262] By the end of 2020, the Canadian press reported that banks had filed more than 100 reports to FINTRAC under Project Shadow, which had in turn referred more than 40 disclosures to law enforcement agencies.[263]

Overall, Canadian PPPs are positively evaluated and have been used as a best practice example,[264] although Canada has also received **criticism** for its strict privacy laws that prohibit sharing tactical information and reversing the flow of information within its PPPs.[265]

[255] As mentioned, this information is not made public and reporting entities do not have access to this metric.
[256] Interview 6, conducted in August 2021
[257] FINTRAC, 2020
[258] Maxwell, 2020
[259] Bradshaw, 2020
[260] Bronskill, 2021
[261] Maxwell, 2020
[262] Maxwell, 2020
[263] Bradshaw, 2020
[264] See Mari, 2017
[265] Trichur, 2021

2.4 United Kingdom

This section presents findings about JMLIT, the PPP aimed at countering financial crime in the UK. It provides an overview of the UK counter-terrorist financing and information-sharing context, followed by a description of the institutional form, legal basis, modus operandi and impact of JMLIT.

2.4.1 Financial information-sharing in the UK

The UK's current response to economic crime includes three collaborative public-private partnerships targeting specific economic crime threats.

The **Joint Fraud Taskforce**, a partnership between banks, law enforcement and government to deal with fraud, which builds on the concept of JMLIT.[266]

The **Dedicated Card and Payment Crime Unit**, aimed at targeting the organised crime groups responsible for card and payment crime. The DCPCU is sponsored by the banking industry. Its partners include the City of London Police, the Metropolitan Police Service, UK Finance and the Home Office.[267]

The **Joint Money Laundering Intelligence Taskforce (JMLIT)**, which enables collaboration between law enforcement, government, the private sector and regulators to target terrorism financing, along with other agreed economic, serious and organised crime threats, and to identify longer term strategic vulnerabilities.[268]

2.4.2 JMLIT

The UK's Joint Money Laundering Intelligence Taskforce piloted in 2015 as the first major public-private Financial Information-Sharing Partnership.[269] It unites the government, law enforcement agencies, regulators and more than 40 banks in a collaborative effort to target economic, serious and organised crime threats and to identify longer term strategic vulnerabilities.[270]

Establishment

JMLIT was established by the NCA in 2015 as a 12-month **pilot**,[271] and was permanently installed in April 2016.

Its establishment was described at length by Bosma (2022). Her research findings show that the establishment of JMLIT required the initiative of several senior members of the public and private

[266] Solicitor General's speech at Cambridge Symposium on Economic Crime, 2017
[267] HM Treasury and Home Office, 2019
[268] National Crime Agency, 2020: p. 29
[269] Redhead, 2021
[270] Maxwell, 2020
[271] Keatinge, 2017

entities, and that **significant barriers** had to be overcome to enable the establishment of JMLIT, particularly building trust and finding an acceptable legal basis.[272]

The **Terrorist Financing Experts Working Group** was added to JMLIT in 2015.

Composition

JMLIT is a partnership between government, regulators, law enforcement, and more than 40 UK and global banks. It includes vetted staff from Barclays, BNP Paribas, Citigroup, Deutsche Bank, JPMorgan, HSBC, Lloyds, RBS, Santander, and Standard Chartered.[273]

JMLIT is located in the National Crime Agency's **National Economic Crime Centre (NECC)**,[274] which coordinates and tasks the UK's response to economic crime and is intended to harness intelligence and capabilities from across the public and private sectors to tackle economic crime in the most effective way. The NECC launched in October 2018 and includes representatives or officers from the NCA, the Serious Fraud Office (SFO), the Financial Conduct Authority (FCA), the City of London Police, HM Revenue and Customs, CPS and the Home Office. It also houses the UK FIU.

JMLIT consists of over 40 financial institutions, the Financial Conduct Authority, Cifas, and five law enforcement agencies: the NCA, HMRC, the SFO, the City of London Police, and the Metropolitan Police Service.[275]

The partnership is structured in **three key components**: an Operational Group, a Strategic Group and an Alerts Service.

The **Operational Group** consists of 13 banks, the National Crime Agency, CIFAS, the Financial Conduct Authority, HMRC, CoL, the Financial Fraud Action UK, and other members as appropriate.[276]

The **Strategic Group** includes expert groups aligned with the priority areas: Trade Based Money Laundering, Money Laundering Through Markets, Organised Immigration Crime and Modern Slavery/Human Trafficking, Bribery and Corruption, Future Threats, and Terrorist Finance.[277] [278]

The **Terrorist Financing Experts Working Group**, part of the Strategic Group, is comprised of over 25 financial institutions, payment services, supervisors, government, law enforcement and civil society partners, Including HM Treasury, Home Office, BEIS, NCA, FCDO, Cabinet Office, and others.

[272] Bosma, 2022
[273] Jaeger, 2018
[274] The Institute of International Finance & Deloitte, 2019
[275] National Crime Agency, sd
[276] Agencia, nd
[277] Agencia, nd
[278] Richiardi, 2018

The **Alerts Service** includes all British Banking Association members, with a particular focus on smaller banks and building societies.[279]

JMLIT is overseen by a Management Board and a Senior Management Team.[280] The Management Board is advised by an Advisory Group chaired by the British Banking Association and a bank member.[281]

Concerning the inclusion of **NPOs**, Transparency International UK is member of the bribery and corruption Experts Working Group.[282] The expansion of JMLIT to similar partnerships with **other sectors**, such as telecoms companies and social media was envisaged by The UK Economic Crime plan in 2019.[283]

Legal basis

JMLIT participants use the data-sharing gateway available to the NCA under **Section 7 of the UK Crime and Courts Act 2013.**[284][285] As opposed to comparable PPPs, JMLIT operates within a common law jurisdiction.[286]

Bosma (2022) offers an analysis of how a legal gateway was found to establish JMLIT. She describes how Section 7 of the UK Crime and Courts Act 2013[287] was repurposed to serve as a legal gateway to enable tactical information-sharing between public and private actors in the JMLIT Operations Group. Bosma's research describes how this gateway would override Privacy law and thus, banks' obligations of confidentiality towards their customers could be suspended. Her research furthermore found that the reinterpretation of the existing rule functioned as a legal and material portal of trust.

The Economic Crime Plan 2019-2022 states the introduction of major recent legislative reforms intended to clarify information-sharing requirements and facilitate information-sharing to tackle economic crime, including the Criminal Finances Act 2017 and the Data Protection Act 2018, which permits the processing of personal data where it is necessary for the purposes of the prevention of crime, subject to certain safeguards.[288]

Objectives

The objectives of JMLIT are described and **defined** in the following ways:

To allow the banking sector to work with law enforcement in line with their regulatory requirements and improve the collective understanding of the money laundering threat **(detect)**, to improve the prioritisation of risks by financial institutions and inform the strengthening of banks

[279] Agencia, nd
[280] Richiardi, 2018
[281] Agencia, nd
[282] Transparency International UK, 2021: p. 27
[283] O'Neill, 2019
[284] Home Office, 2016
[285] Crime and Courts Act (2013), available at https://www.legislation.gov.uk/ukpga/2013/22/contents
[286] Maxwell, 2020
[287] Crime and Courts Act (2013), available at https://www.legislation.gov.uk/ukpga/2013/22/contents
[288] HM Treasury and Home Office, 2019

systems and controls **(protect)**, and to inform the prosecution and disruption of money laundering activity and allow law enforcement to establish a comprehensive understanding of financial information relating to a case **(disrupt)**. [289]

The JMLIT **priority areas of focus** have been described as: Tackling the laundering of the proceeds of bribery and corruption, especially illicit finance from collapsed regimes; tackling trade based money laundering, which includes a focus on illicit money flows hidden behind opaque corporate structures and beneficial ownership; tackling the laundering of the proceeds of human trafficking and organised immigration crime; tackling terrorist financing, which includes a focus on foreign terrorist fighters and international money flows that support terrorist funding.[290]

The Economic Crime Plan 2019-2022 lists 'better information-sharing' as one of its **strategic priorities**. It details the objectives for cross-border information-sharing for JMLIT, aimed at enabling a more thorough understanding of risk, trends and methodologies in relation to economic crime and enable both the public and private sectors to better target their efforts. It proposed for the NECC, with support from HMT, to conduct an international information-sharing pilot linking up JMLIT with foreign public-private partnerships by July 2020.[291]

Practices and procedures

JMLIT is a tool for inter-agency cooperation which operates on both a tactical level, through its operations group, and at a strategic level, through its Expert Working Groups.[292]

The Operations Group is divided in a Banking Sector Operations Group (BSOG) and an Insurance and Investment Sector Operations Group (IISOG), both of which engage in tactical information and intelligence sharing, based on the information-sharing gateway provided by Section 7 Crime and Courts Act 2013.

Information-sharing is undertaken in a **physically co-located hub** equipped with appropriate infrastructure. As opposed to certain other PPPs, JMLIT analysts are based in their home organisations and only convene for meetings.[293] **Vetted representatives** from the public and private sectors meet weekly or monthly to exchange intelligence and analytical findings to support and develop investigations aligned to the JMLIT priorities.[294] In these meetings, live requests for intelligence in the context of law enforcement investigations are shared between member LEAs and the vetted bank representatives. Private sector members of JMLIT are encouraged to refer cases to the Operations Group using an information-sharing gateway. In 2018, the FATF Mutual Evaluation Report reported that the JMLIT Operations Group was briefed on an average of three cases per week by relevant LEAs, some of which may have originated as referrals from JMLIT's private sector members, and that it had accepted and developed 443 cases from law enforcement.[295]

[289] Richiardi, 2018; The Commonwealth, sd
[290] The Commonwealth, sd
[291] HM Treasury and Home Office, 2019
[292] HM Treasury and Home Office, 2019
[293] Chadderton & Norton, 2019
[294] Maxwell, 2020
[295] FATF, 2018: p. 47-48

The information-sharing gateway complements, but does not interfere with, the mandatory obligations imposed by the UK's SAR regime.[296] When participating institutions develop a suspicion of ML/TF in a JMLIT case, they are obliged to submit a SAR to the FIU.[297]

Information-sharing within the Operations Group happens **on a voluntary basis**, at the discretion of its participants, so it is dependent on the co-operation of the requested institution(s). LEAs report broad success obtaining information through these channels, particularly where they have an existing relationship with the requested institution.'[298]

At the **strategic** level, a series of Expert Working Groups focus on **specific threat themes**, including human trafficking and organised immigration crime.[299] Expert Groups operate along thematic lines to identify typologies and emerging risks and transmit this information to the wider financial sector in an accessible way. The key areas of focus for the Expert Groups are based on threats identified in the NRA and key serious and organised crime priorities.[300] The Terrorist Financing Experts Working Group is charged with providing a centralised terrorism financing forum. It was established to support the exchange and analysis of terrorism financing information, with the ability to distribute information to a much wider audience. The group supports thematic pieces of work focused on improving the understanding of threats, risks, typologies and methodologies, in order to improve the detection and disruption of terrorist financing. This is carried out through analytical assessments and projects.[301]

Through JMLIT, LEAs can, **with one request, obtain information from multiple institutions**, which is considered to be an efficient means to develop a comprehensive intelligence picture.[302]

JMLIT provides a new avenue for **enhancing international information-sharing.** Firstly, the UK is championing similar partnerships in other countries and at the European level through the EFIPPP,[303] putting forward JMLIT as an innovative approach and an example of best practice. The UK is also championing public-private partnerships in other countries with the goal of establishing a worldwide network of public-private partnerships which could share information between themselves. For example, two NCA officers were deployed to Australia to work with the Australian FIU (AUSTRAC) on the development of the FINTEL Alliance—an Australian public-private partnership launched in 2015. JMLIT also supported the establishment of Hong Kong's Fraud and ML Intelligence Taskforce, launched in May 2017.[304]

Secondly, LEAs in other countries may submit cases and requests for consideration to JMLIT through the NCA. [305] In 2018, the FATF reported that this feature had not yet been widely used, but, if used regularly, provided scope to enhance international co-operation. The FIU had also initiated a pilot to push appropriate inbound Egmont requests through JMLIT. [306]

296 FATF, 2018: p. 47-48
297 FATF, 2018: p. 51
298 FATF, 2018: p. 152
299 Keatinge, 2017
300 FATF, 2018: p. 47-48
301 HM Treasury & Home Office, 2020: p. 22-23
302 FATF, 2018: p. 51
303 Anti Money Laundering Centre NL , 2020
304 FATF, 2018
305 FATF, 2018: p. 11
306 FATF, 2018

Privacy and proportionality

Concerns have been raised regarding the **privacy implications** of JMLIT operations, as its exchange of detailed information of individual transactions presents a conflict of interest with **data protection requirements**, to be resolved by the legislator. This is said to have slowed the push to model PPPs in other countries after the UK's approach.[307] The concerns mostly centered around JMLIT's compatibility with the General Data Protection Regulation **(GDPR)**. The risk of potential repercussions of GDPR sanctions caused initial reluctance for firms to share information.

However, specific provisions exist within the UK's 2018 Data Protection Act, which address money laundering regulations and enable firms to continue adhering to their duties without violating GDPR. Money laundering falls under the legitimate interest category where it would not be appropriate to seek customers' permission before sharing data.[308]

In the **National Economic Crime plan 2019-2022**, it was acknowledged that, insofar that information being shared between the public and private sectors consists of personal data, such sharing must comply with data protection legislation (the Data Protection Act 2018 and Regulation (EU) 2016/67 – the General Data Protection Regulation) and the Information Commissioner's Office's (ICO) data-sharing code of practice. This is to ensure that the rights of data subjects are protected and their privacy is respected. It furthermore acknowledges that

> "people want and expect law enforcement agencies and private sector firms to stop economic crime, but they also want to know how and why their information is being used. They want to know that it is used responsibly and kept safely, and that they have redress where there is misuse."[309]

It furthermore states the need to consider how appropriate information-sharing can be enhanced, including through the development of guidance, raising awareness of existing gateways, and legislation. This includes considering the regulatory expectations, operational infrastructure, cost involved and culture around information-sharing, as well as concerns relating to data protection, privacy, commercial aspects, anti-competitive behaviour, client confidentiality and privilege. The National Economic Crime Plan also underscores the potential difference in barriers concerning 'voluntary' or 'permissive' information-sharing, as opposed to 'mandatory' information-sharing, such as the SAR regime, and between sharing information internationally as opposed to domestically.[310]

There are some safeguards in place with regards to tactical information-sharing within the Operations group. For instance, LEAs can only request information through JMLIT provided the request is justified, proportionate and necessary.[311]

[307] O'Neill, 2019
[308] Striking the right balance between privacy and fighting financial crime, 2018
[309] HM Treasury and Home Office, 2019
[310] HM Treasury and Home Office, 2019
[311] FATF, 2019

Accountability

JMLIT was established under the Serious and Organised Crime Financial Sector Forum within the NCA, chaired by the Home Office, the British Bankers' Association and the NCA. JMLIT is led by the NCA.[312]

Effectiveness

In contrast to certain other PPPs, JMLIT regularly reports information on its operational impact.[313] However, in a 2021 report, Deloitte mentions **limitations** on how performance data is gathered, and that impact is likely to be significantly understated. Additionally, a number of noteworthy results cannot be disclosed in the public domain for security reasons. Lastly, according to the report, certain aspects are challenging to capture in quantitative data.[314]

JMLIT's operational impact is measured along the **metrics** detailed below. Data relating to terrorism financing are captured within these numbers, but no quantitative data available on JMLITs actions per priority area are available. Qualitative data in the form of individual, high-profile cases relating to TF is discussed at the bottom of this section.

Number of law enforcement investigations

In 2019, it was reported that since its inception, JMLIT has supported and developed over 600 law enforcement investigations.[315] According to the most recent data, that number has since climbed to 950 law enforcement investigations.[316]

Number of arrests made

Between February 2015 and June 2018 (inclusive), 105 arrests[317] were made in connection to JMLIT, among which 63 arrests of individuals suspected of money laundering in the period between May 2016 and March 2017 (inclusive).[318] In 2019, it was reported that since its inception, 150 arrests had been made.[319] With 56 arrests in the period of 2019-2020,[320] as of June 2020, JMLIT had led to 210 arrests.[321] According to the latest numbers, JMLIT has directly contributed to over 280 arrests[322] since its inception.

Number of bank-led investigations into customers

Between May 2016 and March 2017 (inclusive), JMLIT is credited by the NCA with the instigation of more than 1000 bank-led investigations into customers suspected of money laundering,[323] resulting in the heightened monitoring by banks of more than 400 accounts.[324] In 2018, it was

312 Maxwell, 2020
313 Chadderton & Norton, 2019: p 49
314 The Institute of International Finance & Deloitte, 2019
315 HM Treasury and Home Office, 2019
316 National Crime Agency, 2020
317 Maxwell, 2019: p. 6
318 Maxwell & Artingstall, 2017: p. 14
319 HM Treasury and Home Office, 2019
320 National Crime Agency, 2020
321 Nicholson, 2021
322 National Crime Agency, sd
323 Maxwell & Artingstall, 2017: p. 14
324 Jaeger, 2018

reported that since inception and as a direct consequence of JMLIT activity, 3301 bank-led investigations had begun[325] Most recently, that number is up to 6000. [326]

Number of accounts identified which were previously unknown to law enforcement
Between February 2015 and June 2018 (inclusive), 3369 accounts were identified that were not previously known to law enforcement as a result of JMLIT,[327] of which more than 2000 in the period between May 2016 and March 2017 (inclusive)[328]

Amount of criminal funds seized or restrained
Between February 2015 and June 2018 (inclusive), partnership impacts included GBP 12m in suspect criminal assets restrained,[329] of which GBP 7m in the period of May 2016 to March 2017 (inclusive).[330] Other sources claim that by 2018, this number approximated GBP 9m (since JMLIT's inception).[331] By 2019, reporting mentioned the seizure or restraint of over GBP 34m.[332] The period of 2019-2020 saw GBP 3398776 restrained or seized; GBP 9m of cash forfeitures and an additional GBP 9m worth of cash seizures. The NCA also assisted in the seizure of a further GBP 17.6m by other agencies.[333] As of June 2020, JMLIT had led to GBP 56m in assets being seized or restrained.[334] According to the most recent numbers published by the NCA, that number is currently at more than GBP 86m.[335]

Number of Alerts (typology knowledge products)
According to the FATF's Mutual Evaluation Report of the UK in 2018, JMLIT produces flow-on benefits for reporting entities which are not part of the largest institutions or dealing with high-priority cases, through its development of alerts that are distributed to a wider audience. Non-JMLIT banks are reported to have filed SARs based on the information learnt from these alerts.[336]

Between February 2015 and June 2018 (inclusive), 33 alerts (typology knowledge products) had been produced.[337] Currently, over 60 'JMLIT Alert' reports have been shared with the wider financial industry to assist in focusing the identification and implementation of transactional monitoring system queries, in turn helping to mitigate the criminal methodologies used to exploit the UK's financial system[338]

Number of accounts closed
By 2018, JMLIT had led to the closure of over 1563 accounts.[339] In the period 2019-2020, 3740 customers reportedly had their bank accounts closed as a direct result of JMLIT support,[340]

[325] FATF, 2018
[326] National Crime Agency, sd
[327] Maxwell, 2019: p. 6
[328] Maxwell & Artingstall, 2017: p. 14
[329] Maxwell, 2019: p. 6
[330] Maxwell & Artingstall, 2017: p. 14
[331] FATF, 2018
[332] HM Treasury and Home Office, 2019
[333] National Crime Agency, 2020
[334] Nicholson, 2021
[335] National Crime Agency, sd
[336] FATF, 2018: p. 48-52
[337] Maxwell, 2019: p. 6
[338] National Crime Agency, sd
[339] FATF, 2018
[340] National Crime Agency, 2020

although a different report states that 3400 accounts were closed from JMLIT's inception through June 2020.[341]

Improvement in the quality of SARs

Numerous new typologies have been identified, documented and shared across the wider regulated sector through JMLIT.[342] According to the FATF Mutual Evaluation Report, the quality of SARs in some areas has significantly improved as a result. One request by law enforcement agencies through JMLIT can obtain information from multiple financial institutions. SARs that follow such a request are considered to be of a very high standard. [343]

Individual cases

The 2018 FATF Mutual Evaluation Report for the UK cites two specific examples of JMLIT's success. Both are related to terrorism financing matters in response to high-profile terrorist attacks in London in 2017. JMLIT assistance allowed law enforcement to rapidly obtain a full financial picture of the attackers. In relation to one of the attacks, it was established that there was no broader network beyond the three attackers..[344] The FATF concluded that the strong public-private partnership on TF matters, facilitated by JMLIT and a close relationship between the NTFIU and UK financial institutions which has proved effective in practice, is a positive feature of the UK's system.[345]

[341] Jaeger, 2018
[342] The Institute of International Finance & Deloitte, 2019
[343] FATF, 2018
[344] FATF, 2018
[345] FATF, 2018

3. Ethics and PPPs: Recommendations

The previous section has documented four approaches to PPPs, based on information collected through interviews with experts and stakeholders, as well as through desktop research.

In this section, 10 recommendations for future action are presented. Their scope exceeds the case studies described in the previous section. As they are based on an analysis of the case studies, combined with a reading of the wider literature, expert interviews which covered topics beyond the case study countries, and field notes gathered at selected events, they aim to be broadly applicable to PPPs worldwide.

The recommendations in this section are intended to help stakeholders intensify their efforts to bring PPPs into line with ethics, fundamental rights and democratic principles, as they continue their efforts to combat financial crime through PPPs. They speak to the main research questions on ethics, practices and legal frameworks of PPPs. In doing so, these recommendations aim to raise awareness of the work PPPs do, and of the legal and ethical challenges they entail. As there is no one-size-fits-all approach to PPPs, these recommendations are not meant as a comprehensive or exhaustive guide, but are adaptable to each national context.

Recommendation 1: Re-evaluate the place of PPPs in the broader AML/CFT architecture

PPPs are omnipresent in discussions on the future of countering financial crime. They have emerged as a response to negative evaluations of the effectiveness of existing SAR regimes. However, PPPs are currently a **voluntary commitment** on top of existing AML/CFT obligations such as transaction monitoring and customer due diligence.

Interviews revealed that this produces considerable **challenges**. Firstly, there is a risk that the array of CFT instruments a country uses becomes opaque and overly complex.[346] Secondly, **conflicting public and private** roles, responsibilities, and interests may arise when they are no longer clearly separated, such as when banks collaborate with public partners in a PPP on the one hand, even as, on the other, they are subject to penalties from those same public actors for failing to comply with AML/CFT regulations. Thirdly, financial institutions assume ever-greater **financial burdens** when additional features are added to their AML/CFT commitments. Lastly, the impacts on privacy increase, as is discussed in more detail below.

As PPPs mature and develop in various ways, there is a need to review their place in the broader AML/CFT architecture. For instance, there is a lack of clarity on the purpose and **future of PPPs**: Are they meant to complement the SAR system, or to replace it? So that an informed debate on the necessity and legitimacy of PPPs can be had, their effectiveness needs to be evaluated more conclusively, along with **conclusive evidence** on whether PPPs **remedy the deficiencies of the existing system**. There is also the question of whether alternatives to PPPs could achieve the same goal of remedying the shortcomings of the current AML/CFT regime.

[346] Wesseling & de Goede, 2018

The aim of this debate should be to determine how to achieve maximum security impact while minimising burdens and harmful impacts in the fight against financial crime. This requires attention to the effectiveness of the AML/CFT policy architecture in a each country concerned, to the division of responsibilities within each national system, and to the unintended consequences.

Box 6: Recommendation 1: action points

- Acknowledge the financial and practical burdens of additional AML/CFT instruments in fulfilment of legal requirements, on public as well as private actors;
- Critically evaluate the added value of PPPs within the wider AML/CFT architecture. This includes reflection on the balance between added security impact and unintended consequences;
- Investigate competing or conflicting roles and interests of those who participate in PPPs;
- Consider taking bold decisions on the discontinuation of ineffective or inefficient systems in the fight against financial crime.

Recommendation 2: Investigate and mitigate the vulnerabilities of PPPs being used for illegitimate purposes

There is a risk that PPPs can be misused for illegitimate purposes. It is recommended that action be taken to prevent and detect the abuse of information-sharing gateways for illegitimate purposes.

Firstly, the risk of **authoritarian abuses** of AML/CFT standards set by the FATF is gaining urgency, whereby FATF standards are deliberately co-opted and misapplied to suppress journalists, human-rights activists, civil-society actors, NGOs, and those engaged in political dissent.[347] This issue is relevant to authoritarian countries, but equally so in cases where authoritarian tactics are adopted in established democracies.[348]

PPPs are vulnerable to such authoritarian abuses when government or law enforcement personnel use their power for personal gain or out of political motives. This may happen when PPP models that don't have protections in place against authoritarian abuses are applied in authoritarian third countries, as well as when an existing PPP is abused after a change in power.

Interview data indicate that both key forms of information-sharing used in PPPs are vulnerable to authoritarian abuses. Interviewees expressed concerns regarding the potential for **tactical information-sharing** gateways to be abused for such purposes as targeting human-rights activists, civil-society actors, NGOs, or those engaged in political dissent. Tactical information-sharing gateways can be used to circumvent the judicial authorisation that law enforcement agencies standardly need in order to request information from banks. Precisely because they allow for direct requests, that is, without judicial control, of privacy-sensitive personal information about the financial transactions of specific persons, tactical information-sharing gateways can be abused to target specific persons for illegitimate purposes. Interviewees also identified that **strategic information-sharing** can be used to target broader categories of people by formulating typologies and threats based on political motives.

[347] Reimer, 2022
[348] See, for instance: International Institute for Democracy and Electoral Assistance, 2022

Secondly, fieldwork data revealed concerns regarding the risk of **insider threats** as a result of the infiltration of banking personnel or government agencies on the part of those seeking to acquire and abuse confidential information. Interviewees identified various **good practices** regarding measures to mitigate the risk of insider threats. These include limiting access to tactical information to vetted banking personnel who have received security clearance, the use of privacy-preserving technologies used to share information without personally identifying data, the signing of non-disclosure agreements, building trust between partners, gatekeeping which parties are invited to take part in a PPP, and taking cybersecurity measures.

Box 7: Recommendation 2: action points

- Improve the evidence base towards understanding the occurrence of authoritarian abuses of anti-financial crime instruments;
- Identify vulnerabilities of PPPs to insider threats and authoritarian abuses;
- Study whether/how these vulnerabilities can be mitigated and ensure that appropriate measures are implemented in each new and existing PPP;
- Ensure independent oversight and accountability of PPPs at both the national and the supranational levels;
- Empower civil society actors, including NGOs, researchers, and journalists to act as watchdogs;
- Establish channels available to PPP partners and to observers, whereby any actual or suspected abuse or misuse can be reported. Encourage and protect whistleblowers;
- Establish minimum standards for private sector entities participating in a PPP, in terms of having sufficient physical, technical and administrative measures in place such as transparent internal controls, adequate cybersecurity and vetted personnel;
- Monitor the development of PPPs in contexts with high risks of authoritarian abuses;
- Encourage the dissemination of information on good and bad practices regarding the prevention and mitigation of insider threats and authoritarian abuses.

Recommendation 3: Align operations with good governance objectives and ethical principles

Regarding good governance, findings suggest that there is a predominant focus on legal aspects, and a relative lack of attention to ethics. **Guiding ethical principles and good governance objectives** should be prioritised in the design and implementation of PPPs. It is important that PPPs have strong policies in place, as well as an overall cultural orientation towards ethical practice.

Although interviewees were generally aware of the ethical factors involved in the work that PPPs do and of the importance of good governance, fieldwork indicated that there appears to be a tendency to translate PPPs' ethical aspects into legal issues. Attempts are made to address and exhaust ethical issues by ensuring regulatory compliance. However, while a strong legal basis and working within the confines of the law are paramount, legal compliance is only one aspect of good governance for PPPs. A **singular focus on legal aspects** can get in the way of adequate reflection on the risks that PPPs may pose in terms of democratic legitimacy and fundamental rights. Such an approach is too narrow and may produce blind spots. It is recommended that that those who

participate in PPPs engage in **principles-based practices with good-governance objectives**, and that they put a thorough engagement with ethics at the heart of what they do.

As most interviewees pointed out, a one-size-fits-all approach to PPPs is not possible, due to differing national contexts presenting different national capabilities and responding to differing threats. Ethical principles and good governance objectives should therefore be defined at the national level. However, there is room for international cooperation in **setting common standards** in terms of good governance and ethical principles, which can be adaptable to national contexts.

Box 8: Recommendation 3: action points

- Establish an ethics committee within every PPP, tasked with advising on ethical issues, defining good-governance objectives and periodically evaluating the overall ethical impact of the PPP;
- Adopt guiding ethical principles to shape practices and procedures. These principles should cover such themes as privacy, proportionality, accountability, and transparency;
- Define concrete good-governance objectives based on those ethical principles, to be adhered to by public and private partners of the PPP;
- Consolidate guiding ethical principles and good governance objectives in governance documents and terms of reference that set out procedures and practices;
- Conduct a self-assessment regarding ethical aspects and/or get a qualified outside perspective on the strengths of any existing orientation towards ethics, as well as on areas for improvement;
- Clarify expectations at EU level regarding ethical aspects and good governance within PPPs;
- Support outstanding practices regarding ethics and good governance by publicizing and sharing them across PPPs.

Recommendation 4: Establish a solid legal basis prior to the onset of activities

A solid legal basis is key to the establishment of a fully functional PPP.

Interviews and document analysis showed that establishing a legal basis for information-sharing partnerships can be a challenge. Three main kinds of **information-sharing gateways** are utilized to establish a PPP in the observed case studies: i) the repurposing of existing laws; ii) the creation of covenants within the existing legal framework; iii) the creation of new laws that make specific reference to PPPs.

Observations also showed that PPPs tend to start off small or informal, for instance as **pilots**, and grow organically into a more structured partnership. Findings suggest that the timeframe between the start of the partnership as a pilot and its consolidation, is most vulnerable to legal uncertainty. Of particular concern are cases where PPPs engage in tactical information-sharing during the pilot phase, only to solidify the legal basis some years later, when they have matured and taken on a more fully formed structural character.

Various issues can arise. Firstly, the gateway that is created so that public and private partners can share tactical information, **operates at the limits of the law** in some cases.[349] For instance, as Bosma (2022)[350] describes, 'techno-legal gateways' may be created to enable the establishment of PPPs, which entail the stretching of the legal boundaries through creative interpretations of existing laws. Secondly, the absence of a proper legal basis leaves room for **legal uncertainty** about PPPs. Specifically, legal uncertainty around the full competencies of the PPPs and each of its partners[351] may mean that PPPs cannot fully realise their potential, while partners risk **responsibility and liability** for acting without a legal basis. Thirdly, the absence of a clear legal basis also poses risks to the persons whose data are handled and shared by PPPs. For instance, when the PPPs **compatibility with data protection regulations** is not clarified[352] there may be a lack of clarity on how data protection regulations should be applied.

A solid legal basis which **codifies in law** the roles and responsibilities, the purposes and modalities of, the conditions for, the limitations on and safeguards around information-sharing through PPPs, gives **confidence to partners** participating in PPPs, provides **legal certainty** to citizens who are affected by PPPs, and provides **democratic legitimacy** to the PPP.

Box 9: Recommendation 4: action points

- Before the activities of a given PPP start, including during pilot phases, there should be a solid and unambiguous legal basis for establishing a PPP and the activities it plans to engage in;
- Codify PPPs in the law, including the purposes of, the conditions for, the limitations on and safeguards around information-sharing;
- Issue guidance on how existing EU rules apply in the context of Public-Private Partnerships;
- Codify roles and responsibilities of the respective partners clearly. It may be beneficial, in terms of legal clarity, for the legislation to give those who participate in PPPs a clear and specific mandate to engage in information-sharing, as opposed to reinterpreting or repurposing existing laws;
- Suspend any data-sharing activities so long as any legal unclarity regarding the appropriate legal basis for data-sharing or data protection issues within PPPs are not resolved.

Recommendation 5: Limit tactical information sharing to proportionate use

As tactical information-sharing entails the sharing of sensitive personal data between public and private entities without prior judicial authorization, any use of such an information-sharing gateway should be proportionate. Various practices engaged in within PPPs affect the proportionality of operations. For instance, the use of network mapping methods or iterative processes implies the ever greater expansion of networks of associates of suspects which come into view.[353]

[349] Wesseling & de Goede, 2018
[350] Bosma, 2022: p. 145-173
[351] United Nations Office on Drugs and Crime, 2021: p. 83
[352] Mouzakiti, 2020
[353] See Wesseling & de Goede, 2018

Good practice would be to engage in tactical information-sharing only when the conditions of a **twofold proportionality test** applied at two key moments of the tactical information-sharing process are fulfilled.

Firstly, tactical information-sharing should not be engaged in arbitrarily. Judicial authorization should be preferable to tactical information-sharing through a PPP **unless strictly necessary**. In order to ensure proportionate use, any request for information to a private entity through the tactical information-sharing gateway of a PPP, instead of a request made by a LEA following judicial authorization, should be **justified and explainable**.

Secondly, when the tactical information-sharing gateway is used, the **categories of data, contextual information and amount of personal data** that is included in the Request for Information shared by the LEA or FIU with the private entity, should be limited to strictly the minimum necessary amount for the Request For Information to be effective.

The principles of **necessity and data minimisation** should guide all tactical information-sharing, in order to improve proportionality.

Box 10: Recommendation 5: action points

- Clearly define the scope of each PPP's activities. A public-interest test should be applied, and the scope should be defined as narrowly as possible to prevent function creep;
- Apply a proportionality test before each instance of tactical information-sharing. This can be done, for instance, by legal advisors prior to requests for information from the FIU to the financial institutions. Tactical and contextual information provided to the participating private actors should be limited as much as possible, and each request for information should be justified in accordance with the principle of necessity. These decisions should be documented;
- Issue guidance at EU level and at the national level on the categories of data allowed to be shared within a PPP;
- Monitor for disproportionate use of information-sharing gateways through oversight and accountability mechanisms (see below).

Recommendation 6: Preserve the privacy and data protection rights of citizens

The questions of privacy and data protection are important legal and ethical concerns in regard to the AML/CFT regime in general,[354] and for PPPs in particular.[355] Observations show that the question of privacy rights in PPPs is often conflated with the question of compliance with data-protection regulations. It is worth noting that, at the EU level, privacy rights and data-protection rights are commonly recognized as two distinct sets of fundamental rights,[356] both of which need to be protected by PPPs.

Fieldwork revealed two main unresolved **data-protection** issues in regard to PPPs. Firstly, there is some **uncertainty** among stakeholders when it comes to data protection within PPPs. This

[354] Kaiser, 2018
[355] Dehouck & de Goede, 2021
[356] European Data Protection Supervisor, sd

uncertainty poses a barrier for (potential) partners to engage in PPPs with full confidence ('**dare-to-share**'). Secondly, there are disparities among different countries' approaches to PPPs regarding the interpretation of what is allowed within the GDPR. In the absence of EU-level guidance, there is a tendency to operate at the limits of GDPR based on local interpretations whereby the aim is to maximise what PPPs can do within the limits of existing legislation. This varies greatly across EU member states. Consequently, PPPs **move at varying speeds** across the EU, meaning that some PPPs go further by including more categories of partners or sharing tactical information, than others which are operating in a more restrictive legal environment that does not allow for certain kinds of information-sharing.

The data suggests that the predominant view among stakeholders is that the **privacy impact** of PPPs differs from the privacy impact of the SAR regime. In this view, the **targeted approach** of tactical information-sharing through PPPs is considered to have a narrower privacy impact than transaction monitoring. Whereas transaction monitoring has an impact on the privacy of all clients of all reporting entities, PPPs entail a **further-reaching privacy impact on a smaller selection of clients of participating banks**. The interview data suggest that this is viewed by stakeholders as a positive development for privacy protection in the AML/CFT regime. The targeted approach is put forward as more 'privacy-friendly' than transaction monitoring.

However, as one interviewee emphasised, PPPs are currently not used as an alternative to transaction monitoring, but as an addition to it. As long as this is the case, they constitute an expansion of the privacy impact of the AML/CFT regime as a whole. Consequently, if we consider the **cumulative privacy impact** of PPPs within the AML/CFT regime, PPPs do not make AML/CFT more privacy friendly. On the contrary, they are one more way in which the AML/CFT regime affects citizens' privacy. Therefore, so long as they are used as an addition to preexisting AML/CFT instruments, it is misleading to present PPPs as an improvement on privacy.

The question of privacy was voiced as a concern by all interviewed stakeholders. In all studied PPPs, action was taken to address the privacy impact. Examples are the application of a **proportionality test** prior to information-sharing, the development of **Privacy-Preserving Technologies**, and conducting a **Privacy Impact Assessment**.

Box 11: Recommendation 6: action points

- In the interest of legal clarity, and to ensure the protection of the data-protection rights of EU citizens, regulatory guidance is needed at EU level to address the question of Data Protection in relation to PPPs.[357] The European Data Protection Board is the competent body to issue guidance on unresolved Data Protection issues in regard to PPPs;[358]
- Action should be taken to limit the privacy impact of PPPs. Participants in each PPP should assess which aspects of its day-to-day operations have a privacy impact, and should define good-governance objectives to address them in accordance with best practice. This can be done by conducting a Privacy Impact Assessment;
- Encourage the development of privacy-preserving and privacy-enhancing technologies.

[357] For an academic discussion of data protection issues in relation to PPPs, see for instance the work of ParTFin at Tilburg University: https://research.tilburguniversity.edu/en/projects/public-private-partnerships-on-terrorism-financing
[358] European Commission, 2022: p. 1)

Recommendation 7: Enhance transparency of PPPs

The analysis indicates that there is considerable **room for improvement** regarding transparency of PPPs.

Varying degrees of transparency were observed in the PPP case studies. Whereas some PPPs publish reports on their activities, others do not. At the time of data collection, none of the studied PPPs had a dedicated website or a public point of contact. Publicly available information on PPPs is scattered across the participating banks or is not available at all. Alternatively, it is available through media reports or annual reports by the FIU. In the countries studied for this report, relatively little public debate in newspapers and other media outlets took place when the PPPs were set up. Information on the amount of data that is processed through a PPP, the number of interventions made, and the number of ongoing investigations, which are vital pieces of information when it comes to evaluating the effectiveness, proportionality and impact of a PPP, was publicly reported on in none of the studied PPPs.

According to interviewees, the **lack of transparency** may be due to a number of factors. Firstly, some interviewees expressed the view that a certain level of **secrecy** is necessary because sensitive information regarding TF or ML investigations is involved. Secondly, in one case, a bank employee participating in a PPP argued that, because PPPs involve private sector partners, they do not have a **democratic imperative** to be transparent about their activities. Thirdly, interviewees expressed the view that in light of **limited resources and capacity**, transparency was not made a priority.

However, in order to **foster public debate** on PPPs and for citizens to exercize their rights, more information on what PPPs do, how they work, how citizens are affected by them, and the impact they have, should be made publicly available. Secrecy should be reduced to a minimum, and should be justified bearing in mind the guiding principles of accountability and transparency.

Box 12: Recommendation 7: action points

- Each PPP should publish regular performance reports or annual reports on its activities, on its objectives, on the results it achieves, on its impact and on how it evolves;
- Allocate resources to the creation of a communication strategy, so that consideration can be given to how best to maximise transparency and openness. The operative principles here should be transparency and accountability, so that recourse to secrecy is had only where strictly necessary;
- Raise awareness of the work PPPs do, their impact and their ethical challenges;
- Make governance documents and terms of reference publicly available and easy to retrieve;
- Present a full picture in reporting so as to not only communicate successes but also harmful impacts or unintended consequences and future directions;
- Promote international cooperation in aggregating this information into a comparative view;
- Challenge the argument that because PPPs involve private partners, they do not have a democratic imperative to be transparent about their activities.

Recommendation 8: Systematically evaluate the impact of PPPs

The research indicates that the impact of PPPs is not being adequately evaluated due to a lack of suitable and harmonised metrics to measure their effectiveness and unintended consequences.

Observations show that while all studied PPPs measure the effectiveness of their operations, each uses **different metrics**. This makes it challenging to make **meaningful comparisons**. Moreover, not all PPPs measure the **unintended consequences** of their operations. At the time of data collection, none of the PPP case studies had published any information that showed that they measure the unintended consequences or harmful impact of their activities.

On the one hand, the data shows a **generally strong belief** among stakeholders that PPPs are more effective than transaction monitoring in the fight against the financing of terrorism and other financial crimes, and that they are a necessity in the AML/CFT architecture. On the other hand, interviews also revealed that many **difficulties in measuring the effectiveness** of PPPs render it challenging to substantiate this belief. The following challenges were identified: firstly, some outcomes are considered valuable but intangible or difficult to measure (e.g., building trust between partners). Secondly, it could take years for an activity a PPP engages in to produce a measurable result, from the time information is shared until an investigation is concluded or leads to a conviction. Thirdly, it is difficult to establish a clear cause-and-effect relation between the activities a PPP engages in and a reduction in financial crime. Lastly, depending on the regulations, banks may not be allowed to receive feedback on whether a SAR they have filed in response to information that has been shared within the PPP, was useful to the FIU or to law enforcement.

As a result, there is **a lack of high-quality, consistent and comparative data** on the impact of PPPs. Based on this data, the effectiveness of PPPs cannot be conclusively demonstrated and it remains quite unclear what exactly the added benefit or disadvantage of PPPs is.

As PPPs mature and move beyond the pilot and early-development stages, an in-depth study should be conducted into the impact they have produced thus far. It is important that **not only successes** be evaluated and reported on, but also harmful impacts, mistakes and unintended consequences.

Box 12: Recommendation 8: action points

- Acknowledge the difference in national contexts, threats and circumstances which influence the impact of PPPs in any given country;
- Acknowledge the difficulty in capturing the impact of PPPs in statistics due to their indirect, long-term or immaterial impact;
- Produce and publish data which enables stakeholders and observers to assess PPPs' performance and impact;
- Investigate ways to develop a harmonised set of metrics to measure the impact of PPPs, so as to allow for a comparative view. That in turn will make it possible to draw broader conclusions regarding the effectiveness and legitimacy of PPPs in general;
- Offer transparency to actors engaged in oversight, as well as researchers, citizens, and civil-society actors.

Recommendation 9: Task dedicated agencies with oversight of PPPs and ensure that PPPs are held accountable

Findings suggest a lack of oversight and accountability of PPPs at the national and supranational levels.

Oversight of the activities PPPs engage in is necessary to monitor and enforce good-governance objectives such as transparency, proportionality, and the protection of privacy. PPPs need to ensure oversight, keeping in mind the guiding principle of accountability. Accountability means that decisions are reported on and explained, and that they can be sanctioned.[359]

Firstly, oversight of PPPs **at the national level** was not present in all case studies. PPPs require a supervisor tasked with monitoring their activities, as appropriate in the national context. National governments should establish formal oversight mechanisms for new and existing PPPs. Secondly, There is currently no oversight at **EU or supranational level**. There is no formal body tasked with oversight of PPPs at the EU level and the FATF does not specifically monitor PPPs as part of its MERs as it is not a mandatory feature of the AML/CFT architecture.

The absence of oversight is sometimes explained by a reliance on horizontal relationships between PPP partners, whereby trust plays a key role. However, while trusted relations are a key factor in forming PPPs, they do not offer adequate safeguards to ensure accountability, so they should be complementary to oversight mechanisms.

Box 13: Recommendation 9: action points

- Develop and define the parameters of meaningful accountability in the context of PPPs. Such accountability measures should include monitoring and evaluation by data-protection authorities, as well as obligations to report to expert bodies and institutional actors at the national and supranational levels, or parliamentary reporting.[360]
- Establish and/or designate the appropriate agency to be tasked with impartial oversight at different levels of governance, i.e. at the national level, EU-level and supranational level.
- Mandate independent observers with periodically conducting audits or continually monitoring PPPs, particularly regarding their compliance with ethical standards and good governance objectives. These observers could be consultants, legal advisors, or representatives of NGOs;
- Promote self-assessment by PPPs;
- Continuously raise awareness and hold PPPs accountable for their impact on financial crime as well as their unintended consequences and their impact on privacy and other human rights.

[359] Center of Expertise for Good Governance, 2022
[360] Curtin & de Goede, 2023

Recommendation 10: Ensure that citizens can exercise their rights where they are affected by PPPs

PPPs should put in place effective measures to protect the rights of those whose personal data is processed. They should create appropriate means for citizens to exercise their rights where these are affected by PPPs, including ensuring the **right of redress** in case a PPP makes a mistake or difficulties regarding financial access are encountered by persons whose data was shared in a PPP.

PPPs share personal and contextual data on citizens who are **not (yet) suspects** in a criminal investigation. These citizens have come to the attention of a LEA or FIU in the context of a financial crime investigation. This may, for instance, be the result of a **mapping of networks** between persons based on transactions.[361] Through a tactical information-sharing gateway, the personal data of these citizens can be shared with financial institutions as part of a Request for Information.

Fieldwork revealed concerns that tactical information-sharing through PPPs can be considered as a way to **circumvent criminal procedures**, by bypassing the judicial authorisation needed for law enforcement agencies to obtain data from financial institutions regarding specific persons or companies. In this view, tactical information-sharing in the framework of PPPs entails a suspension of **procedural safeguards** for the persons whose data is handled.

Moreover, persons whose data has been processed through tactical information-sharing are not informed that they have come to the attention of police authorities or financial investigators. They are not informed that their data are being shared with financial institutions through the tactical information-sharing gateway, or that their networks have been mapped. They are not made aware when problems regarding **financial access** that they encounter, are the result of their being the subject of an RFI within a PPP. As such, the data-protection **rights to information, correction and redress**, as codified in the GDPR, are suspended by PPPs. The activities of PPPs do not allow for these rights to be exercised in practice. In the studied countries, there were no mechanisms for informing individuals that their data has been processed within a PPP, and there seemed to be no way for citizens to access, review, or correct the data shared within a PPP in practice.

Interview data suggests that this may be due to a conflict between citizens' rights and **tipping-off** provisions, and to a lack of clarity on **data protection rights' compatibility** with PPPs.

Box 14: Recommendation 10: action points

- Establish redress mechanisms so that citizens who have been impacted by the activities of a PPP can exercise their rights;
- The European Data Protection Authority should provide guidance on which circumstances can justify suspending EU data-protection rights, and establish clear limits on the suspension of those rights by PPPs;
- Each PPP should create a central point of contact for enquiries and complaints (e.g., an ombudsperson) and publish information that details the rights of citizens which are impacted by the activities of the PPP, including how citizens can find appropriate means of redress if they believe their rights have been affected. They should also create a mechanism or point of contact for citizens to exercise their right to know.

[361] Wesseling & de Goede, 2018

4. Conclusion

This study contributes to a better understanding of public-private partnerships for financial information-sharing in the context of fighting financial cime, by providing insight into their legal and ethical aspects. It discusses four approaches to PPPs, and offers recommendations applicable to PPPs worldwide.

This report has documented four PPPs through document analysis and research interviews conducted between April 2021 and November 2022. It was already known that PPPs were developing in as many different ways as there were national contexts. This research clearly indicates that this variety is reflected in the ways in which good governance and ethical issues are dealt with in PPPs. It has found that ethics and good governance within PPPs are characterised by a variety of ways to ensure legal certainty, and by different practices regarding privacy, oversight, accountability, transparency, and the protection of citizens' rights. The data also suggests that a singular focus on legal aspects is generally prioritized, to the detriment of the development of ethical frameworks within PPPs.

In addition to a descriptive discussion of four case studies, this report therefore offers ten recommendations aimed at drawing attention to ethics within PPPs. The recommendations revolve around good governance and harmonising ethically oriented approaches across PPPs. These recommendations are intended to strengthen the democratic legitimacy of PPPs, the compatibility of their activities with fundamental rights, and safeguards against abuse.

We encourage policymakers as well as stakeholders involved in PPPs to implement the proposed recommendations in order to intensify their efforts to bring PPPs in line with fundamental rights, democratic principles and ethical practice, as they continue their efforts to combat financial crime through public-private partnerships.

Annex 1: Sources cited

Agencia. (n.d.). *Multi Agency Collaboration*. Retrieved from British Virgin Islands Financial Services Commission: https://www.bvifsc.vg/sites/default/files/L015MultiAgencyCollaboration-AMENDED.pdf

Amicelle, A., & Iafolla, V. (2018). Suspicion-in-the-making: Surveillance and Denunciation in Financial Policing. *Suspicion-in-the-making: Surveillance and Denunciation in Financial Policing, 58*(4), 845-863.

Anti Money Laundering Centre NL. (2020, October 26). *AMLC in Europol Financial Intelligence Public Private Partnership Steering Group (EFIPPP)* . Retrieved from Anti Money Laundering Centre NL: https://www.amlc.eu/amlc-in-europol-financial-intelligence-public-private-partnership-steering-group-efippp/

Banken.nl. (2018, July 12). *Justitie en banken werken samen tegen terrorisme*. Retrieved from Banken.nl: https://www.banken.nl/nieuws/21003/justitie-en-banken-werken-samen-tegen-terrorisme

Biggin, D., & Lervik, F. (2021). *Striking Back Against Financial Crime: Closer public-private sector collaboration is needed to fight financial crime in the Nordics*. PA Consulting.

Bosma, E. (2022). Banks as security actors. Countering terrorist financing at the human-technology interface (Unpublished doctoral dissertation). University of Amsterdam.

Bradshaw, J. (2020, December 28). Scotiabank follows money to detect signs of child sexual exploitation. *The Globe and Mail*.

Bronskill, J. (2021, July 30). Telltale transactions help financial intelligence centre combat sex trafficking. *The Canadian Press*.

Canada NewsWire. (2021, February 22). *Scotiabank's Financial Access Program Marks First Anniversary with New Partnerships*. Retrieved from Bloomberg: https://www.bloomberg.com/press-releases/2021-02-22/scotiabank-s-financial-access-program-marks-first-anniversary-with-new-partnerships

Center of Expertise for Good Governance. (2022). *12 Principles of Good Governance*. Retrieved from Council of Europe: https://www.coe.int/en/web/good-governance/12-principles#{%2225565951%22:[11]}

Chadderton, P., & Norton, S. (2019). *Public-Private Partnerships to Disrupt Financial Crime: An Exploratory Study of Australia's FINTEL Alliance*.

Commissie voor Justitie en Veiligheid. (2020, December 29). Verslag van een wetgevingsoverleg: Regels omtrent gegevensverwerking door samenwerkingsverbanden (Wet gegevensverwerking door samenwerkingsverbanden) .

Council of the European Union. (2022, June 29). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010*. Retrieved from Council of the European Union: https://data.consilium.europa.eu/doc/document/ST-10507-2022-REV-1/en/pdf

Crisp, W. (2018, December 29). Financial Crime: the new battlefield. *The Telegraph*.

Curtin, D., & de Goede, M. (2023). Bits, Bytes, Searches, and Hits: Logging-in Accountability for EU Data-led Security. In D. Curtin, & M. Catanzariti, *Data at the Boundaries of European Law*. Oxford University Press.

Danske Bank. (2020, May 27). *Danske Bank joins new initiative with Swedish police to fight financial crime.* Retrieved from Danske Bank: https://danskebank.com/news-and-insights/news-archive/news/2020/27052020

De Bont. (2019, November 29). *Convenant Pilot Serious Crime Taskforce.* Retrieved from De Bont Spot On: https://www.debontspoton.nl/wwft-tucht/convenant-pilot-serious-crime-taskforce/

Dehouck, M., & de Goede, M. (2021). *Public-Private Financial Information-Sharing Partnerships in the Fight Against Terrorism Financing: Mapping the Legal and Ethical Stakes.* Amsterdam: University of Amsterdam.

DG FISMA – Unit D2. (2021, July 23). *Guidance on the rules applicable to the use of public-private partnerships in the framework of preventing and fighting money laundering and terrorist financing.* Retrieved from Preventing money laundering and terrorist financing – EU rules on public-private partnerships (PPPs): https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13152-Preventing-money-laundering-and-terrorist-financing-EU-rules-on-public-private-partnerships-PPPs-_en

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. (n.d.). Retrieved from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017L0541

Ellis, C., Pantucci, R., de Roy van Zuijdewijn, J., Bakker, E., Gomis, B., Palombi, S., & Smith, M. (2016). *Lone-Actor Terrorism: Final Report.* London: RUSI.

European Commission. (2020, May 13). *Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing 2020/C 164/06.* Retrieved from Official Journal of the European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0513%2803%29

European Commission. (2022). *Commission Staff Working Document on the use of public-private partnerships in the framework of preventing and fighting money laundering and terrorist financing.* Brussels.

European Data Protection Supervisor. (sd). Data Protection. Retrieved from European Data Protection Supervisor: https://edps.europa.eu/data-protection/data-protection_en#:~:text=The%20Right%20to%20Data%20Protection,personal%20data%20(Article%208).

FATF. (2017). *Anti-money laundering and counter-terrorist financing measures - Sweden, Fourth Round Mutual Evaluation Report.* Paris: FATF.

FATF. (2018). *Anti-money laundering and counter-terrorist financing measures - Sweden, 1st Enhanced Follow-up Report & Technical Compliance Re-Rating.* Paris: FATF.

FATF. (2018). *Anti-money laundering and counter-terrorist financing measures United Kingdom: Mutual Evaluation Report.* FATF.

FATF. (2019). *Best Practices on Beneficial Ownership for Legal Persons.*

FEC. (n.d.). Retrieved from Financieel Expertise Centrum: https://www.fec-partners.nl/nl#:~:text=Het%20Financieel%20Expertise%20Centrum%20(FEC,van%20deze%20sector%20te%20versterken.

FEC. (n.d.). *Organisatie.* Retrieved from Financieel Expertise Centrum: https://www.fec-partners.nl/nl/organisatie/organisatie

Financial Intelligence Unit - Nederland. (2021, February 11). *FIU-Nederland treedt samen met de grootbanken op tegen witwassen en terrorismefinanciering.* Retrieved from Financial Intelligence Unit - Nederland: https://www.fiu-nederland.nl/nl/fiu-nederland-treedt-samen-met-de-grootbanken-op-tegen-witwassen-en-terrorismefinanciering

Financieel Expertise Centrum. (2020). *FEC Jaarplan 2020.*

Financieel Expertise Centrum. (2021). *FEC Jaarplan 2021.* FEC.

Finansdepartementet. (2022, April 28). *Lagstiftning för bekämpning av penningtvätt och finansiering av terrorism*. Retrieved from Regeringskansliet: https://www.regeringen.se/artiklar/2017/09/lagstiftning--for-bekampning-av-penningtvatt-och-finansiering-av-terrorism/

FINTRAC. (2020). *FINTRAC Annual Report 2019-20*.

FINTRAC. (n.d.). *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. Retrieved from Financial Transactions and Reports Analysis Centre of Canada: https://www.fintrac-canafe.gc.ca/act-loi/1-eng

FIU-Nederland. (2020). *FIU-Nederland Jaaroverzicht 2019*. FIU-Nederland.

Forsman, M. (2020). 30 years of combating money laundering in Sweden and internationally – does the system function as intended? *Sveriges Riksbank Economic Review, 1*, 24-55.

Guldåker, N., Hallin, P.-O., Nilvall, K., & Gerell, M. (2021). Crime Prevention Based on the Strategic Mapping of Living Conditions. *ISPRS International Journal of Geo-Information, 10*(11), 719.

HM Treasury & Home Office. (2020). *National risk assessment of money laundering and terrorist financing 2020*.

HM Treasury and Home Office. (2019). *Economic Crime Plan 2019-22*. HM TReasury and Home Office.

Hoikkala, H. (2020, May 28). *Swedish Dirty Money Affair Brings Bankers Closer to Police*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2020-05-27/sweden-s-money-laundering-affair-brings-bankers-closer-to-police#:~:text=Swedbank%20AB%2C%20which%20was%20fined,better%20at%20fighting%20financial%20crime.

Home Office. (2016). *Criminal Finances Bill - Information Sharing: Impact Assessment*.

International Governance & Compliance Association. (2021, February). *Current Trends in AML Webinar Transcript*. Retrieved from International Governance & Compliance Association: https://igca.org/current-trends-in-aml-webinar-transcript/

International Institute for Democracy and Electoral Assistance. (2022). *Global State of Democracy Report 2022*. Stockholm: International Institute for Democracy and Electoral Assistance.

Jaeger, J. (2018, September 12). *New SFO director will leverage compliance officers' expertise*. Retrieved from Compliance Week: https://www.complianceweek.com/new-sfo-director-will-leverage-compliance-officers-expertise/2146.article

Josefsson, V., & Wrigley, S. (2021, January 22). *Sweden Moves Anti-Money Laundering Efforts Forward with Public-Private Partnership*. Retrieved from FRA: https://www.forensicrisk.com/sweden-moves-anti-money-laundering-efforts-forward-with-public-private-partnership/

Kaiser, C. (2018). *Privacy and Identity Issues in Financial Transactions: The proportionality of the European anti-money laundering legislation*. [Thesis fully internal (DIV), University of Groningen]. University of Groningen.

Keatinge, T. (2017). Following the Financial Footprints: New approaches to Disrupting Human Trafficking and Modern Slavery. *The European Review of Organised Crime, 4*(2), 128-146.

Kouwenhoven, H. (2018, July 6). Banken ontdekken driehonderd mogelijke 'terrorismebetalingen'. *NRC Handelsblad*, p. 1.

Kreling, T. (2019, August 7). Waarom moet ABN Amro haar particuliere klanten onderzoeken? En wat dient er precies onderzocht te worden? *De Volkskrant*.

Mari, J. (2017, December 12). *Project Protect: An In-Depth Review of the Public-Private Partnership to Combat Human Trafficking in Canada*. Retrieved from ACAMS Today: https://www.acamstoday.org/project-protect-combat-human-trafficking-in-canada/

Market News Publishing. (2021, July 29). Stepping up fight to end human trafficking with new funding for innovative programs. *Market News Publishing*.

Maxwell, N. (2019). *Expanding the Capability of Financial Information-Sharing Partnerships*. RUSI.

Maxwell, N. (2020). *Survey report: Five years of growth in public–private financial information-sharing partnerships to tackle crime*. Future of Financial Intelligence Sharing Programme (FFIS).

Maxwell, N., & Artingstall, D. (2017). *The Role of Financial Information-Sharing Partnerships in the Disruption of Crime*. RUSI.

Menou, B. (2021, January 28). Le blanchiment dans le viseur des banques suédoises. *L'AGEFI Hebdo*, p. 13.

Menou, B. (2021, February 11). Les banques suédoises patrouillent avec la police contre le blanchiment. *L'AGEFI Hebdo*, p. 39.

Mijnheer, D. (2019, February). Publiek-private samenwerkingen bij de bestrijding terrorismefinanciering . *Tijdschrift voor Compliance*, pp. 5-11.

Milne, R. (2021, November 24). SEB chief attacks failure to halt dirty money. *Financial Times*, p. 8.

Ministerie van Justitie en Veiligheid. (2020, January 9). *Factsheet Convenanten*. Retrieved from Kenniscentrum Wetgeving en Juridische zaken: https://www.kcwj.nl/sites/default/files/Factsheet_Convenanten.pdf

Ministry of Finance. (2022, April 21). *Combatting money laundering and terrorist financing*. Retrieved from Government offices of Sweden: https://www.government.se/government-policy/financial-markets/combatting-money-laundering-and-terrorist-financing/

Mouzakiti, F. (2020). Cooperation between Financial Intelligence Units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive. *New Journal of European Criminal Law, 11*(3), 351–374.

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2020, October 15). *Dreigingsbeeld NCTV: Aanslag Nederland voorstelbaar, dreiging vooral van eenlingen*. Retrieved from NCTV: https://www.nctv.nl/themas/contraterrorisme/nieuws/2020/10/15/dreigingsbeeld-nctv-aanslag-nederland-voorstelbaar-dreiging-vooral-van-eenlingen

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2021, April 14). *Dreigingsbeeld NCTV: Aanslag in Nederland voorstelbaar, geen aanwijzingen voorbereiding aanslag*. Retrieved from NCTV: https://www.nctv.nl/actueel/nieuws/2021/04/14/dreigingsbeeld-nctv-aanslag-in-nederland-voorstelbaar-geen-aanwijzingen-voorbereiding-aanslag

National Crime Agency. (2020). *National Crime Agency Annual Report and Accounts 2019/2020*.

National Crime Agency. (n.d.). *National Economic Crime Centre*. Retrieved from National Crime Agency: https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre

Nederlandse Vereniging van Banken. (2019, December 17). *Banken en autoriteiten bundelen krachten; samen sterk tegen witwassen*. Retrieved from Nederlandse Vereniging van Banken: https://www.nvb.nl/bank-wereld-online/banken-en-autoriteiten-bundelen-krachten-samen-sterk-tegen-witwassen/

Nederlandse Vereniging van Banken. (2021, February 11). *Nieuwe publiek-private samenwerking in Fintell Alliance - "Nieuwe boost voor aanpak witwassen"*. Retrieved from Nederlandse Vereniging van Banken: https://www.nvb.nl/bank-wereld-online/nieuwe-publiek-private-samenwerking-in-fintell-alliance-nieuwe-boost-voor-aanpak-witwassen/

Nederlandse Vereniging van Banken. (2022, April 12). *Position paper: Information sharing in the fight against money laundering*.

Nicholson, D. (2021, March 26). *Information fusion in the fight against financial crime*. Retrieved from UK Finance: https://www.ukfinance.org.uk/news-and-insight/blogs/information-fusion-fight-against-financial-crime

Office of the Privacy Commissioner of Canada. (2012, March). *PIPEDA and the Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. Retrieved from Office of the Privacy Commissioner of Canada: https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/financial-transaction-reporting/faqs_pcmltfa_01/#003

O'Neill, D. (2019, August). Privacy fears slow spread of UK-style data-sharing to combat money laundering. *Euromoney*.

O'Neill, D. (2019, August). Privacy fears slow spread of UK-style data-sharing to combat money laundering. *Euromoney*.

O'Neill, D. (2019, July). UK dirty money plan stirs 'policy capture' debate. *Euromoney*.

Openbaar Ministerie. (n.d.). *Samenwerking in strijd tegen terrorismefinanciering belangrijk*. Retrieved from Openbaar Ministerie: https://www.om.nl/onderwerpen/terrorismefinanciering/samenwerking-in-strijd-tegen-terrorismefinanciering

Pilieci, V. (2013, October 25). Personal data gathered, despite warning; Privacy commissioner says FINTRAC collects information without valid reason. *Ottawa Citizen*.

Prince George Citizen. (2009, November 18). Privacy alarm; Watchdog worried government agency collecting too much financial information. *Prince George Citizen*.

Proceeds of Crime (Money Laundering) and Terrorist Financing Act (S.C. 2000, c. 17). (n.d.). Retrieved from Justice Laws Website: https://laws-lois.justice.gc.ca/eng/acts/P-24.501/index.html

Redhead, M. (2021). *The future of transaction monitoring: better ways to detect and disrupt financial crime*. Swift Institute.

Reimer, S. (2022, November 2). *Authoritarian Abuses: The Weaponisation of Anti-Financial Crime*. Retrieved from RUSI: https://www.rusi.org/explore-our-research/publications/commentary/authoritarian-abuses-weaponisation-anti-financial-crime

Richiardi, C. (2018). *Anti-Financial Crime Partnerships*. Retrieved from Finance Latvia Association: https://www.financelatvia.eu/wp-content/uploads/2018/11/Workshop-2-presentations-23112018.pdf

Rosenberg, E., & Wester, J. (2019, July 5). 'Wij kunnen met 4.500 man justitie bijstaan, maar wel vanuit vertrouwen'. *NRC Handelsblad*.

SEB and banks intensify cooperation with police in fight against money laundering. (2020, May 20). *Governance, Risk & Compliance Monitor Worldwide*.

SEB. (n.d.). *Cooperation takes the fight against money laundering to the next level*. Retrieved from SEB: https://sebgroup.com/about-us/our-role-in-society/corporate-citizenship/samlit

Soetenhorst, B. (2020, February 13). *'Overheid mist slagkracht bij toezicht op terreurfinanciering'*. Retrieved from Het Parool: https://www.parool.nl/nieuws/overheid-mist-slagkracht-bij-toezicht-op-terreurfinanciering~b5359620/?referrer=https%3A%2F%2Fwww.google.com%2F

Solicitor General's speech at Cambridge Symposium on Economic Crime. (2017, September 5). *Impact News Service*.

Striking the right balance between privacy and fighting financial crime. (2018, November 6). *Impact News Service*.

Sveriges Riksbank. (2021, January 21). *Nordic-Baltic countries engage the IMF to conduct an analysis of cross-border money laundering and terrorist financing risks in the region*. Retrieved from Sveriges Riksbank: https://www.riksbank.se/en-gb/press-and-published/notices-and-press-releases/notices/2021/nordic-baltic-countries-engage-the-imf-to-conduct-an-analysis-of-cross-border-money-laundering-and-terrorist-financing-risks-in-the-region/

Swedbank. (2021, January 19). *Banks and the Swedish Police Authority formalize AML-cooperation.* Retrieved from Swedbank: https://news.cision.com/swedbank/r/banks-and-the-swedish-police-authority-formalize-aml-cooperation,c3269613

Swedish Bankers' Association. (2019, October 29). *Förslag om utökade möjligheter till informationsdelning i syfte att stärka arbetet mot penningtvätt och finansiering av terrorism.*

Swedish Police Authority. (2021). *National Risk Assessment of Money Laundering and Terrorist Financing in Sweden 2020/2021.*

Swedish Police Authority. (2021). *The Financial Intelligence Unit Annual Report 2020.* Swedish Police Authority.

The Commonwealth. (n.d.). *Public-private information sharing partnerships to tackle money laundering in the finance sector: the UK experience.*

The Institute of International Finance & Deloitte . (2019). *The global framework for fighting financial crime: Enhancing effectiveness & improving outcomes.*

The Swedish National Council for Crime Prevention. (2021). *Financing of terrorism: A study of countermeasures.*

Transactie Monitoring Nederland. (n.d.). *Wat is TMNL?* Retrieved from Transactie Monitoring Nederland: https://tmnl.nl/

Transparency International UK. (2021). *Annual Impact Report and Accounts 2020-2021.*

Trichur, R. (2021, February 22). Ottawa must better counter money laundering; OPINION. *The Globa and Mail.*

United Nations Office on Drugs and Crime. (2021). *Compendium of promising practices on Public-Private Partnerships to prevent and counter trafficking in persons.* Vienna: United Nations.

van der Veen, H., Heuts, L., & Leertouwer, E. (2019). *National Risk Assessment Terrorismefinanciering 2019.* Wetenschappelijk Onderzoek- en Documentatiecentrum.

Van Genugten, J. (2019, December 13). *Why does Scandinavia have so many money laundering scandals?* Retrieved from The FCPA Blog: https://fcpablog.com/2019/12/13/why-does-scandinavia-have-so-many-money-laundering-scandals/

Wesseling, M., & de Goede, M. (2018). *Beleid Bestrijding Terrorismefinanciering: Effectiviteit en Effecten.* Amsterdam: Universiteit van Amsterdam - Amsterdam Institute for Social Science Research.

Annex 2: Data collection

The table below provides a list of conferences and webinars attended by researchers where field notes were gathered.

Box A.2.1: Field sites		
Webinars		
Date	Title	Organiser
July 2020	CTF Online Symposium No. 2: Terrorism, Tech and Finance.	CRAAFT/RUSI
October 2020	De-risking – Where is the Balance Between Risk and Inclusion?	AML RightSource
November 2020	Risk Assessments in 2020 and Beyond	AML RightSource
December 2020	Academic Roundtable with FATF President Dr. Marcus Pleyer	RUSI
January 2021	ICCT Live Briefing: How Terror Evolves	ICCT
March 2021	Illicit financial flows 2021	Chatham House
March 2021	FinCrime World Forum 2021	Fintrail
November 2021	Women in Fincrime Summit	AML Intelligence
November 2021	Shared Risk Intelligence: A centralized, open database to share risk information between entities	FinScan
January 2022	FinCrime Global	GRC World Forums
January 2022	New Dawn in Compliance: Moving Compliance Functions from Defense to Offense	Data Protection World Forum
January 2022	CTF Online Symposium No. 8: The EU and Counter-Terrorism Financing	RUSI/ Project CRAAFT
February 2022	CTF Online Symposium No. 9: State Funding, Malign Influence and Terrorism Financing: Challenges for Europe	RUSI/ Project CRAAFT
February 2022	PrivSec Global	GRC World Forums
February 2022	Terrorism Financing: How to assess, investigate and report on TF risks.	GRC World Forums
February 2022	POLITICO Live's 2022 Finance Summit	POLITICO
March 2022	PrivSec Risk In Focus	GRC World Forums
April 2022	Extracting Value from your Data, Capitalize on Insights not Privacy	Duality
April 2022	The Future of Economic Crime Policing	CFCS

May 2022	FinCrime Focus: Anti-Money Laundering	GRC World Forums
July 2022	Public-Private Partnerships on Terrorism Financing Roundtable on Data Protection Scenarios	PartFin
In-person events		
Date	Title	Organiser
June 2022	Surveillance Studies Network Conference 2022	Surveillance Studies Network (Erasmus University Rotterdam)
October 2022	The 2022 Conference of Partnerships	FEC, RUSI FFIS
November 2022	Reassessing the Financing of Terrorism in 2022	RUSI Europe, Project CRAAFT