Occasional Paper

Making Information Flow
Instruments and Innovations for Enhancing Financial Intelligence

David Carlisle
Making Information Flow
Instruments and Innovations for Enhancing Financial Intelligence

David Carlisle
Over 180 years of independent defence and security thinking

The Royal United Services Institute is the UK’s leading independent think tank on international defence and security. Its mission is to be an analytical, research-led global forum for informing, influencing and enhancing public debate on a safer and more stable world.

Since its foundation in 1831, RUSI has relied on its members to support its activities, sustaining its political independence for over 180 years.

London | Brussels | Nairobi | Doha | Tokyo | Washington, DC

The views expressed in this publication are those of the author(s), and do not reflect the views of RUSI or any other institution.

Published in 2016 by the Royal United Services Institute for Defence and Security Studies.

This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

RUSI Occasional Paper, August 2016. ISSN 2397-0286 (Online).
# Contents

Acknowledgements v  
Foreword vii  
*Tom Keatinge*

Executive Summary ix  

**Introduction** 1  

I. Broadening and Deepening Networks 9  
Expanding and Embedding Public–Private Exchanges 9  
Enabling Private–Private Exchanges 15  
Expanding Official Collaboration 18  

II. Navigating SAR Confidentiality 21  
Enterprise-Wide Sharing 22  
Cross-Border FIU Notifications 25  
Clarifying ‘Tipping Off’ 26  

III. Harnessing Technology 29  
Integrating and Embedding Systems 29  
Funding 32  

IV. Summary and Conclusions 35  

About the Author 37
Acknowledgements

The author thanks Tom Keatinge, Inês Sofia de Oliveira and David Artingstall of RUSI’s Centre for Financial Crime and Security Studies for providing the opportunity to conduct this research, and for their ongoing guidance and encouragement. He is grateful to the Publications staff at RUSI for their hard work and support, and he is especially appreciative of the numerous experts with whom he has consulted in researching the topic of information sharing for lending their insight, opinions, time and advice.
Foreword

Tom Keatinge

THE IDEA THAT greater information sharing will lead to better outcomes in tackling terrorism, human trafficking, grand corruption and other forms of illicit activity has become widely accepted among global leaders, law enforcement and policy-makers. Yet precisely how this ‘idea’ can be effectively implemented remains elusive.

Nascent national and transnational efforts exist to address this challenge, facilitated by initiatives such as those led by the UK’s Joint Money Laundering Intelligence Taskforce or the Egmont Group of Financial Intelligence Units. Yet despite these initiatives, financial information sharing failures are often revealed as being central to the inability of law enforcement and security services to disrupt terrorist and criminal activity. Furthermore, even though an immense architecture has been created that requires the private sector to share information related to perceived suspicious activity with the authorities, information sharing barriers and inefficiencies are allowed to persist.

Following on from the recently published Centre for Financial Crime and Security Studies Occasional Paper ‘Challenges to Information Sharing: Perceptions and Realities’ that considered the legal ‘art of the possible’ and identified how changes in legislation could be made that enabled more effective information sharing, this latest paper offers concrete and practical recommendations as to how countries and transnational organisations should address the continued operational failings created by a lack of information sharing.

At its heart, this paper emphasises the extent to which the effective exploitation of financial intelligence could empower both the public and private sectors to collaborate and contribute to the identification and disruption of financial crime. Some critical issues need to be addressed if this goal is to be achieved, issues that this paper seeks to explore and illuminate for policymakers, law enforcement and private sector actors alike.
Executive Summary

IMPROVED SHARING OF financial intelligence (FININT) is necessary to protect the international community from terrorism, human trafficking, grand corruption, tax evasion and other illicit activity.

Terrorists, organised criminals and the corrupt operate on a global scale and move funds across borders rapidly. With access to specific and current information about illicit financial activity, law enforcement agencies, regulators and financial institutions can detect and act against these threats. Yet public and private sector stakeholders are often unable to share FININT in a sufficiently timely manner to disrupt illicit networks.

Governments, international institutions and the private sector are developing important new instruments to facilitate more frequent and rapid FININT sharing. These efforts include establishing collaborative public–private FININT partnerships, increasing the frequency of official exchanges between governments and investing in new technological platforms. However, further innovations are necessary to allow the public and private sectors to achieve the level of information sharing required to counter evolving security threats successfully.

This Occasional Paper advances the debate on how best to enhance FININT sharing. It examines ongoing efforts to develop solutions, explores a variety of approaches for improving existing instruments and offers additional ideas for consideration. Its primary observations are as follows:

- Most existing FININT sharing arrangements are limited in scope, in terms of both the number of participants involved and the quality and frequency of exchanges.
- Several countries have developed important domestic models for collaboration and are working to enhance their scope and efficiency. In particular, the UK’s Joint Money Laundering Intelligence Taskforce (JMLIT) stands as a model for targeted exchanges of actionable FININT between the public and private sectors. However, most countries continue to rely on inefficient and outdated approaches to information sharing.
- Information sharing between national financial intelligence units (FIUs) is the key method for sharing FININT internationally. A number of countries have sought to expand information sharing between their respective FIUs. The Egmont Group of FIUs remains the focal point for international FIU collaboration. However, procedural and technical inefficiencies at times hinder FIU-driven information exchanges, which are often only bilateral, limiting countries’ ability to tackle broader regional or global threats.
- The US has taken an innovative approach to FININT sharing by making it a priority of its broader national security intelligence collection. This allows the US to share FININT

1. The Toronto-based Egmont Group is a network of FIUs from more than 150 countries with the aim of enabling information sharing among its members and promoting the development of more effective FIUs. For additional information see: <http://www.egmontgroup.org/about>.
with a wide range of stakeholders through a variety of intelligence and networking channels. Most other countries rely exclusively on their FIUs for collaboration with global partners, and consequently face constraints from the resource and networking limitations of their FIUs.

- Existing practices and standards relating to the confidentiality of suspicious activity reports (SARs) create inefficiencies and inhibit the ability of stakeholders to act in a timely and comprehensive manner against threats.
- A number of countries have undertaken steps to address inefficiencies associated with SAR confidentiality standards, but these efforts have been generally limited in scope and scale. Significant global barriers remain with respect to the ability of financial institutions to disclose important SAR data with international branches and affiliates. This hinders financial institutions in managing financial crime risks internally.
- Financial institutions also continue to face restrictions in reporting that they have filed a SAR in one jurisdiction to a government in another jurisdiction where they also have a filing obligation. This creates barriers to international law enforcement co-ordination.
- In recent years, the public and private sectors have developed a number of important technological innovations to facilitate information sharing while ensuring the integrity of sensitive personal data. These initiatives offer a promising solution for managing the tension between data privacy and enhancing FININT.
- The most promising technological solutions are still not widely available to public and private sector participants, who continue to rely on outdated systems.

Based on the observations above, this Occasional Paper offers the following recommendations:

**Expand and Embed Public–Private Exchanges of FININT**

- Countries should establish domestic collaborative task forces that facilitate the timely exchange of information between law enforcement agencies, regulatory bodies and financial institutions both on specific investigative targets and on broader threats of money laundering and terrorist financing.
- Countries that utilise or develop public-private collaborative task forces should place these arrangements on a more permanent footing. To address the range of financial crime risks they face, countries should also ensure that collaborative arrangements encompass all relevant financial institutions and law enforcement agencies, and target an appropriate range of business lines and product types.
- Governments should also establish streamlined domestic mechanisms for regularly communicating information to financial institutions about strategic financial crime risks and typologies.
- At the international level, governments should explore the potential for bilateral and multilateral platforms that enable public and private sector stakeholders to share information on money laundering and terrorist financing risks across jurisdictions. For example, regional public–private partnerships could involve close cross-border co-ordination among law enforcement agencies and financial institutions on high-risk threats such as terrorism and human trafficking.
Enable the Exchange of FININT Within the Private Sector

- Governments should enable and endorse collaborative exchanges of FININT within the private sector. Industry-based arrangements should be expansive in their membership. They should also offer financial institutions safe harbour from liability for disclosure of sensitive information, subject to specific conditions that ensure the integrity of customer data. Where possible, these networks should be multijurisdictional.

Expand Official Collaboration

- Where possible, governments should expand official bilateral information sharing arrangements so that they become multilateral in scope. This should include increased collaboration among multiple FIUs on either specific investigations or the development of strategic analysis.
- International bodies, and in particular the Egmont Group of FIUs, should facilitate more frequent multilateral information sharing exchanges relating to specific thematic threats. These could include, for example, terrorist financing, the financial flows around human trafficking, the laundering of the proceeds of corruption and other forms of criminal financial activity.
- Governments should increase the sharing of financial information outside of the traditional FIU arrangements. In particular, they can accomplish this by integrating FININT into broader intelligence gathering and sharing channels.

Enable Greater Enterprise-Wide Sharing of FININT

- Partner governments, working in collaboration with standard-setting organisations such as the Egmont Group and the Financial Action Task Force (FATF),\(^2\) should accelerate efforts to harmonise SAR confidentiality requirements and enable greater sharing of SARs within multinational financial enterprises.
- Many governments worry about the impact of more permissive SAR sharing on the integrity of domestic SAR regimes. Where significant concerns persist, governments should make high-level political commitments to explore the potential for reducing barriers to wider cross-border sharing while upholding commitments to meaningful standards of confidentiality and data protection.
- Governments that do not already do so should undertake efforts to enable domestic financial institutions to share SARs with overseas branches and affiliates. Such arrangements should feature strong safeguards and clear conditions to protect the integrity of customer information.

---

\(^2\) The Paris-based FATF is an intergovernmental organisation that sets globally recognised anti-money laundering/counter-terrorist financing (AML/CTF) standards. Its Recommendations form the basis of countries’ AML/CTF efforts, which the FATF monitors to ensure effective implementation. For additional information see: <http://www.fatf-gafi.org/about/whoweare>.
• In countries that already permit some degree of international enterprise-wide sharing, governments should review existing frameworks to ensure they can maintain an appropriate balance between necessary permissiveness and confidentiality requirements.

Enable Cross-Border Notifications to FIUs

• Partner governments, working in collaboration with organisations such as the Egmont Group and the FATF, should seek to enable financial institutions to notify multiple FIUs in other jurisdictions about SAR filings when related to common investigative targets. As with enterprise-wide sharing, these arrangements should feature strong safeguards and clear conditions to protect the integrity of customer information.

Expand Access to IT Systems

• Governments should promote and facilitate expanded access to IT platforms. For example, those bilateral and multilateral information sharing platforms currently in use could be extended to new countries.
• Similarly, governments should encourage private sector-driven initiatives to make shared IT solutions available to a broader population of financial institutions.

Prioritise IT Platforms

• Integrating state-of-the-art technologies should be a key feature of any effort to develop information sharing arrangements. Technology should not be an after-thought. Information sharing arrangements suffer when governments attempt to implement arrangements without appropriate IT platforms being in place.

Encourage Technological Innovation

• Governments should provide additional funding to enhance existing information sharing technologies and to develop new, improved IT platforms that facilitate bilateral and multilateral exchanges.
• Governments and financial institutions should engage in public–private funding partnerships to generate innovative IT solutions.
Introduction

In April 2016, the president of the Financial Action Task Force (FATF), Je-Yoon Shin, said to a collection of public and private sector financial crime experts gathered at the UN:

[Intelligence agencies and law enforcement often hold information on the individuals involved in terrorist attacks before those events. Better and timelier sharing of this information ... could help detect and disrupt attacks before they happen ... Countries also need to make sure that mechanisms are in place to facilitate the exchange of information between domestic authorities, the private sector and international counterparts.]

It is, of course, important that senior officials acknowledge that barriers to the flow of financial intelligence (FININT) are a significant international security risk. The FATF and other expert organisations are undertaking critical studies to identify existing legal barriers that prevent fluid FININT sharing. However, policy-makers must now begin implementing practical solutions to allow intelligence on terrorist financing and other significant illicit finance threats to flow more freely both within countries and across borders.

Doing so will undoubtedly prove challenging and controversial. Countries’ different legal and regulatory structures pose a challenge to the harmonisation of efforts across borders. Public concern over data privacy, and the public and private sectors’ legal obligation to secure that data, creates scepticism that information sharing arrangements can ever be global in scope. Establishing new legislative authorities, and amending and expanding existing laws, is a time-consuming and often politically unappealing task. Thus, while widespread consensus exists about the need for greater information sharing, concrete action is often slow to arrive.

Despite these challenges, there are three key thematic areas where policy-makers can concentrate their efforts to expand FININT collaboration.

Broadening and Deepening Networks

First, at both the national and international levels, stakeholders should use collaborative FININT networks more widely and more frequently.

To date, FININT generation at the national level has relied largely on traditional Suspicious Activity Report (SAR) regimes. While national SAR processes are still a critical aspect of global anti-money laundering/counter-terrorist financing (AML/CTF) efforts, they are often time-

---

Making Information Flow

consuming, resource inefficient and based in ‘silos’. Traditional SAR regimes often do not lend themselves to rapid exchanges of information between different bodies about specific high-priority threats that require urgent attention. In a world where criminals can transfer funds rapidly across borders, more dynamic and integrative exchanges of FININT are essential to enable security services to disrupt threats.

Increasingly, governments are looking to collaborative forums, such as thematic task forces, that allow public and private sector actors to exchange information on certain high-priority security concerns in real time. These forums do not replace SAR regimes and traditional law enforcement methods; instead, they complement them and enhance countries’ abilities to track and act against illicit networks.

Collaborative forums established to date, however, are still largely in their infancy, and have in many cases operated on a one-off or limited-time basis. To keep pace with global threats, public–private FININT partnerships must become a permanent feature of national and international AML/CTF efforts and should be available to a wider range of participants.

In addition to facilitating real-time collaborative forums between law enforcement agencies and financial institutions, governments have an important role to play in empowering financial institutions to share information with peers on a continual basis. The concept of expanding private–private financial information sharing is becoming increasingly important. When private sector actors can share information with one another more fluidly, they are able to develop a more complete picture of customers and transactional activity. This allows them to make better decisions about how to manage their businesses and enables them to provide law enforcement agencies with more detailed, robust SARs.

However, there are at present few available means through which financial institutions can reliably exchange intelligence with peers on money laundering and terrorist financing risks. Private–private partnerships are therefore infrequent. This is unfortunate, as industry players collectively possess troves of valuable data that could prove mutually beneficial in meeting AML/CTF obligations. Collaborative forums that allow private industry to play a more proactive role in detecting and combating money laundering and terrorist financing are therefore critical.

Similarly, international exchanges of FININT between countries are often inadequate for addressing priority threats. International collaboration has traditionally taken place through bilateral exchanges between countries’ financial intelligence units (FIUs). While valuable, bilateral exchanges are often not broad enough in geographic scope to address the risks posed by pressing transnational threats such as terrorism and corruption.

Navigating SAR Confidentiality

A second priority is for governments to acknowledge the constraints that SAR confidentiality places on information sharing. A key principle of international AML/CTF efforts is that the existence of a SAR filing must remain confidential to avoid ‘tipping off’ the subject of a SAR that
it is under investigation. In many jurisdictions, financial institutions therefore may not disclose to their overseas branches and other affiliates that they have filed a SAR in their home country. They also generally face prohibitions on informing an FIU in one jurisdiction that they have filed a SAR in another.

SAR confidentiality, however, presents an intelligence gathering challenge. If a financial institution could share SARs with its overseas branches, it would offer its corporate networks a more complete picture of suspected illegality; similarly, if a financial institution could notify its home country’s FIU that its overseas branch had filed a SAR in another jurisdiction, each countries’ law enforcement agencies could co-ordinate joint efforts more fluidly.

**Harnessing Technology**

Third, the public and private sectors must advance efforts to integrate technological solutions into information sharing arrangements.

In the EU, FIUs have collaborated to develop an important information sharing architecture that facilitates a multilateral FIU exchange network. Similarly, in the US, private sector firms are developing IT solutions to assist them in the sharing of FININT with peers. However, while gaining increasing visibility, these solutions are not yet widely available.
Box 1: Two Models of Information Sharing.

This paper argues that information sharing can become more dynamic through a number of instruments and innovations. Figure 1 provides a simple illustration of how domestic SAR regimes and international information exchanges often occur today. In many countries, FININT sharing between financial institutions is infrequent and fragmented, if it occurs at all (A). Financial institutions report SARs in silos to the domestic FIU (B), which makes that information available to law enforcement agencies seeking information (C). Public sector feedback to and interaction with the private sector may occur through issuing production orders or subpoenas, or through occasional typologies reports (for example, detailed, formal studies that describe specific money laundering and terrorist financing methods) (D), but this interaction is sporadic. Official collaboration with foreign FIUs is often limited to bilateral exchanges with other countries, which operate using similar domestic models (E).

Conversely, a model of FININT exchange that adopts many of the recommendations in this Occasional Paper can offer more fluid, integrated information exchanges, which can in turn lead to higher quality, actionable FININT. Figure 2 offers an illustration of the proposed process.

In this model, domestic financial institutions share information and collaborate in working groups to generate FININT (A). They report SARs directly to the FIU, but interactions with the FIU are more direct and frequent, and feedback from law enforcement agencies via the FIU is more targeted and specific, creating a ‘two-way street’ (B). Individual financial institutions also have bilateral information sharing arrangements with law enforcement agencies, which enhances SAR reporting (C). The public and private sectors engage in ongoing, collaborative task force initiatives that bring together a range of parties to share information (D). Participants of the task force convey the lessons learnt to the broader industry (E).

The domestic FIU has the ability to share information multilaterally with all three foreign FIUs in the figure (F), which have also developed their own regional FIU collaboration framework (G). Each country has its own local information sharing network that resembles the home country’s domestic framework (H).

Domestic financial institutions also share information, including SARs, with branches of their enterprise networks located abroad (I). Finally, official FININT exchanges occur via bilateral or multilateral intelligence agency networks (J).
**Figure 1:** First Model of Information Sharing.

**LE:** Law enforcement

**FIU:** Financial intelligence unit

**FI:** Financial institution
Figure 2: Second Model of Information Sharing.

Domestic

LE: Law enforcement
FIU: Financial intelligence unit
FI: Financial institution
Aims, Method and Structure

This Occasional Paper aims to contribute to the accelerating international discussion about improving the sharing of information on money laundering and terrorist financing. It draws on a small but growing body of literature on the subject, including academic articles, industry white papers and publicly available information provided by governments about their efforts to expand information sharing. This paper also draws on the author’s discussions held between February and June 2016 with more than a dozen experts with experience in both the public and private sectors. This includes individuals with experience at FIUs, financial institutions, industry groups, law enforcement agencies and IT development groups.

A significant number of the examples in this paper relate to the UK and US, where many of the most advanced information sharing projects operate; however, the author has aimed to include examples from other countries and regions as well. The confidential, sensitive nature of many of the information sharing arrangements discussed in this paper presents a methodological challenge: in many instances, the only source of information about their relative effectiveness is the public statements of participants; details of these arrangements’ outputs and operations are often not open to public scrutiny. Furthermore, many of the arrangements and methods discussed in this paper have not undergone independent testing. This is particularly true of those that have come into operation in the past two or three years.

Measuring what makes one information sharing arrangement ‘better’ or ‘more effective’ than another presents another challenge. However, there are several general concepts this paper relies on to assess the relative merits of various information sharing arrangements and methods. Examples include:

- The strength of data safeguards.
- The degree to which information sharing arrangements ensure efficient resource allocation.
- The ability of the methods used to increase the speed of information sharing.
- The ability of information sharing methods to reduce barriers to networking and communication.
- The scalability of information sharing arrangements (that is, the extent to which the methods used can extend to other jurisdictions or additional participants).
- The number and significance of arrests or other disruptions to illicit activity that result from the sharing of information.

This paper does not aim to identify every legal and policy challenge that countries might encounter in implementing information sharing programmes; rather, its focus is to identify a range of practical solutions to improve information sharing that are achievable in the near-to-medium term. Not all of the potential solutions this paper offers will be appropriate for all countries. A hybrid approach is both practical and advisable. This paper aims to highlight the importance of the three thematic areas outlined above: broadening and deepening networks; navigating SAR confidentiality; and harnessing technology. These themes could serve as
foundations upon which policy-makers can base their efforts to make information sharing work. The specific recommendations offered are not prescriptive, as stakeholders could develop a wide variety of potential solutions to achieve policy aims consistent with the broader thematic areas.

This Occasional Paper is divided into three sections addressing each of the thematic areas noted above. It concludes with a summary of key observations and conclusions.
I. Broadening and Deepening Networks

FOCUSED, COLLABORATIVE NETWORKING is essential to produce FININT that can lead to the disruption of security threats. To generate actionable and relevant FININT, financial institutions require up-to-date indications of the security priorities of law enforcement agencies, and details of the methods of criminals and terrorists. Similarly, law enforcement agencies require timely access to specific and detailed data from the private sector about the financial activity of criminals and terrorists. Information sharing must therefore be formalised, focused and ongoing in order to disrupt security threats and to ensure the integrity of the financial system. To this end, governments and the international community more broadly should pursue the following priorities:

• Expanding and embedding public–private exchanges.
• Enabling private–private exchanges.
• Expanding official collaboration.

These three concepts are examined in detail below.

Expanding and Embedding Public–Private Exchanges

When the FATF enshrined SAR reporting as a foundation of global AML/CTF principles in 1989, the concept of public–private information sharing was still relatively simple: if a financial institution suspected illicit activity, it filed a SAR with its FIU, which would make that information available to law enforcement; law enforcement could in turn use that information to support its investigations. The process cast financial institutions as the producers of FININT, FIUs as aggregators and facilitators, and law enforcement agencies as consumers. With distinct roles and segregated responsibilities, governments felt they had designed SAR regimes that could enable a straightforward process for identifying and disrupting illicit activity.

When implemented globally, however, this process has often been inefficient and insufficient for tackling certain threats. The public sector relies on the private sector to file SARs, but in many cases financial institutions do not have adequate information from law enforcement agencies about the nature of criminal threats, and therefore are unable to generate specific, actionable information about the threats of most concern to law enforcement agencies. Furthermore, financial institutions often do not hear the outcomes of investigations that rely on the information they provide in SARs, which hinders their ability to allocate resources effectively to identify illicit activity. If the quality of SARs suffers, the ability of FIUs to carry out their function in analysing and distributing SAR data diminishes as well. Law enforcement agencies will, in turn, lack access to timely and detailed information to support their investigations. The results
of these trends are national-level regimes that lack a genuine sense of partnership among the private and public sectors that could enhance the quality of the information shared.

Recently, ideas about best practice for information sharing have evolved significantly. Public and private sector stakeholders recognise that information sharing must be more formalised and, above all, more precisely designed to enable genuine collaboration in the detection and disruption of evolving threats. Information sharing must not be ‘bottom-up’ or channelled from financial institution to FIU to law enforcement; rather, FININT generation must be an integrative process of continual exchange and learning. In this light, several models of public–private partnership have emerged in recent years that aim to deepen collaboration and improve the quality of FININT.

One of these models features information sharing task forces. This model aims to bring together representatives from law enforcement, regulatory agencies and the private sector to exchange information on specific financial crime threats. It achieves this aim in one of two ways: either by sharing intelligence on specific individuals and entities subject to investigation; or by collaborating to produce detailed typologies studies that provide participants with a better understanding of criminal methods and trends. Task forces operate on the premise that the day-to-day operations of SAR regimes and ongoing law enforcement activities, while critical, tend to cast too wide a net to enable rapid responses to certain security problems. Task forces offer an advantage by focusing participants’ attention on co-ordinating responses to specific high-priority threats.

The AML/CTF task force that has received the greatest public attention of late is the UK’s Joint Money Laundering Intelligence Taskforce (JMLIT). The JMLIT became fully operational in February 2015 at the start of a year-long pilot programme, drawing together the UK’s law enforcement agencies and financial institutions to analyse ‘information and expertise in the public and private sectors to better understand the true scale of money laundering and the methods used by criminals to exploit the UK’s financial system’. Its mandate sets out the following intended outcomes:

- Assisting the private sector in prioritising risks.
- Improving participants’ collective understanding of emerging threats.
- Facilitating targeted law enforcement action.
- Allowing participants to learn from one another’s practices.

At the centre of the JMLIT model is the Operations Group which focuses on tactical intelligence sharing among public and private sector participants. The Operations Group aims ‘to fill
intelligence gaps where suspected money laundering crosses multiple financial institutions'.

Its membership includes the National Crime Agency (NCA) – which houses the UK’s FIU – HM Revenue and Customs (HMRC), the City of London Police, Fraud Action UK and other law enforcement bodies as well as ten of the UK’s largest financial institutions.  

Drawing on its broad information sharing authority under the 2013 Crime and Courts Act, the NCA acts as the focal point for sharing intelligence among the Operations Group’s participants. The NCA is able to share information derived from a variety of sources – including law enforcement information, intelligence derived from SARs and other methods – related to specific investigative targets of law enforcement concern. The banks can use this information regarding suspected individuals and entities to search their internal systems for relevant information, which they can then bring back to the Operations Group to build a more complete picture of financial activity than can be achieved through traditional SAR processes. This enables the JMLIT to function as a ‘two-way street’ and expedites the information sharing process relating to specific, high-priority threats. Both law enforcement agencies and financial institutions can use the intelligence derived to dedicate resources to addressing these operational targets. 

The Operations Group is not a substitute for the SAR regime; rather, its purpose is to provide law enforcement and the private sector with a clearer picture of the end-to-end illicit activity of specific investigative targets. Financial institutions’ broader risk management efforts can also benefit, as lessons learnt from operational collaboration can prompt internal compliance groups to enhance their own procedures and policies. At the national level, the UK has used


4. Ibid., p. 7. Specifically, the Operations Group’s membership includes: the NCA’s Economic Crime Command and National Intelligence Hub; HMRC; City of London Police; Cifas; Barclays; Santander; Standard Chartered; RBS; HSBC; BNP Paribas; Citigroup; Nationwide; Lloyds Bank; and the Post Office.

5. Section 7(1) of the ‘Crime and Courts Act 2013 (UK)’ permits that, ‘A person may disclose information to the NCA if the disclosure is made for the purposes of the exercise of any NCA function’, while Section 7(3) permits that ‘Information obtained by the NCA in connection with the exercise of any NCA functions may be used by the NCA in connection with the exercise of any other NCA function.’


8. Horlick, speech given during a UN joint open briefing of the Counter-Terrorism Committee and the 1267/1989/2253 ISIL (Da’esh) and Al-Qaida Sanctions Committee.


10. Horlick, speech given during a UN joint open briefing of the Counter-Terrorism Committee and the 1267/1989/2253 ISIL (Da’esh) and Al-Qaida Sanctions Committee.
the exercise to identify potential legislative changes to improve not just information sharing, but the effectiveness of the country’s AML/CTF regime as a whole.\textsuperscript{11}

In addition to these tactical FININT sharing arrangements implemented through the Operations Group, the JMLIT includes a Strategic Group that is run by an industry group, the British Bankers’ Association (BBA), and whose participants include law enforcement agencies and 25 financial institutions.\textsuperscript{12} Whereas the Operations Group focuses on the targeted sharing of sensitive intelligence, the Strategic Group shares non-sensitive information in order to develop typologies, threat trend assessments and other strategic products. The broader public and private sectors can draw on this information to understand four high-priority threat areas: bribery and corruption; trade-based money laundering; immigration crime and human trafficking; and terrorist financing.\textsuperscript{13} The aim of the Strategic Group is to enable the public and private sectors to ‘horizon scan’ for threats to the UK financial system related to these criminal activities.\textsuperscript{14}

Law enforcement and private sector participants have lauded the JMLIT for producing important, concrete outcomes that facilitate their ability to act against criminal networks.\textsuperscript{15} According to the Home Office and HM Treasury:

As of February 2016, the JMLIT pilot has directly contributed to law enforcement operations, including eleven arrests and restraint of £558,144 of criminal funds. Over 1,700 bank accounts linked to suspected criminal activity have been identified, 261 have been closed, and 517 are subject to heightened monitoring by the banks. Twelve alerts have been issued to the financial sector to raise awareness of threats.\textsuperscript{16}

As a model for task force-type arrangements, the JMLIT offers features that other jurisdictions may find appealing. It accelerates the intelligence sharing process in a manner that is resource efficient and risk-based. By drawing together a significant number of participants from both the public and private sectors, the JMLIT enables trust building and genuine collaboration, and offers a forum for members to provide real-time feedback to one another. Without feedback from their peers, public and private sector actors remain unaware of the genuine value of the information they share – a problem that generates resource inefficiencies and wasted effort.\textsuperscript{17}

\begin{itemize}
\item \textsuperscript{13} JMLIT, ‘Introduction to the Joint Money Laundering Intelligence Taskforce (JMLIT Toolkit)’, p. 8.
\item \textsuperscript{14} Allen, ‘Uniting to Tackle Financial Crime’.
\item \textsuperscript{15} Kochan, ‘How Law Enforcement is Partnering Up with Banks in AML fight’; Horlick, speech given during a UN joint open briefing of the Counter-Terrorism Committee and the 1267/1989/2253 ISIL (Da’esh) and Al-Qaida Sanctions Committee.
\item \textsuperscript{16} Home Office and HM Treasury, Action Plan for Anti-Money Laundering and Counter-Terrorist Finance, p. 15.
\item \textsuperscript{17} Horlick, speech given during a UN joint open briefing of the Counter-Terrorism Committee and the 1267/1989/2253 ISIL (Da’esh) and Al-Qaida Sanctions Committee.
\end{itemize}
Due to its initial status as a pilot programme, the JMLIT also offered participants the opportunity to learn how to share information in a responsible and genuinely collaborative way. This is important because practising information sharing helps to identify inefficiencies and to identify and then cement best practice.

Participants of the JMLIT’s Operations Group attest to the value of having security-cleared private sector representatives on the task force. The provision of security clearances by governments to the staff of financial institutions has been controversial since the 9/11 Commission advised against it in 2004. On the one hand, allowing the staff of financial institutions access to classified intelligence could help them to act on specific law enforcement concerns; on the other hand, this creates a risk of security breaches. More recently, however, some experts have advocated extending security clearances to individuals at financial institutions to allow for targeted FININT generation. Dennis M Lormel, who led the FBI’s counter-threat finance efforts after 9/11, has suggested that the public sector should aim ‘to legally provide security clearances to select personnel in financial institutions ... to identify account or transactional information associated with terrorists.’

As a pilot programme, the JMLIT therefore offers an example of a partnership involving cleared private sector personnel that generates real results.

However, it may be difficult to replicate the JMLIT model in some jurisdictions. The type of broad information sharing authority afforded to the NCA may prove a difficult political sell in many countries. Indeed, despite the authority of the NCA, both public and private sector participants in the JMLIT reportedly expect to be the subject of litigation related to the disclosure of customers’ personal data. The UK may therefore require new legislation to enable the JMLIT to operate beyond a pilot basis.

In addition to having only been a pilot thus far, the JMLIT’s membership has focused to date on large financial institutions – primarily banks – and therefore has not extensively involved other parts of the financial sector, such as small- and medium-sized money service businesses, asset management firms and the gambling and gaming sectors. To this end, the Home Office has recommended that the JMLIT operate on a permanent footing with an expanded membership.

19. Author’s discussions with industry experts, February and June 2016.
20. Horlick, speech given during a UN joint open briefing of the Counter-Terrorism Committee and the 1267/1989/2253 ISIL (Da’esh) and Al-Qaida Sanctions Committee.
However, the question of how best to expand its membership presents a challenge – one that countries larger than the UK might find particularly difficult. The US, which hosts a far greater number of financial institutions operating across 50 states and under a complex regulatory regime, might struggle to develop a representative national-level platform. Even in the UK, the challenge remains to ensure that the JMLIT remains of an appropriate scale. Making the JMLIT permanent could create a resourcing pressure for firms seeking regular representation in the forum.26

Task forces are not the only option for enhancing public–private partnerships and, in some contexts, may not be the most appropriate model. In certain cases, law enforcement agencies may have concerns about suspected illicit financial activity at a single institution, or may be handling sensitive information that is inappropriate for disclosure to a wider group of participants. In such instances, close bilateral relationships between law enforcement agencies and individual financial institutions may be most effective in enabling targeted operational exchanges. The FBI has reportedly relied on bilateral operational arrangements to address national security threats. Indeed, since 9/11, the FBI has used information from foreign intelligence sources to work with specific contacts in the financial industry to track suspects’ live transactions.27

These bilateral collaborative relationships allow law enforcement and financial institutions to act upon threats in the most deliberate manner possible. They ensure efficient, concentrated resource allocation and enable law enforcement agencies to manage the distribution of sensitive information. One concern, however, is that such bilateral relationships may be perceived as creating competitive advantages for those financial institutions that work with law enforcement. They would also present a resourcing challenge for law enforcement agencies if carried out on a wide scale.28 Task forces, by contrast, allow governments to initiate intelligence-driven information exchanges across a group of several institutions simultaneously.

A final, notable approach to public–private collaboration is the use of streamlined mechanisms that allow the public sector to inform a very broad spectrum of private sector participants about threats.

In the UK, the BBA facilitates an industry-wide information alert programme, the Financial Crime Alerts Service (FCAS), as part of the JMLIT.29 The BBA collects information from the NCA and eleven other UK law enforcement agencies to provide financial institutions across the broader financial sector with up-to-date information on emerging financial crime threats.

26. Ibid.
27. John S Pistole, testimony before the House Committee on Financial Services, Subcommittee on Oversight and Investigation, 24 September 2003.
as well as strategic and thematic reports. The FCAS aims to streamline the dissemination of non-classified information about financial crime typologies and red flags related to a number of security threats – in particular terrorist financing, money laundering, bribery and corruption, cyber- and e-crime, and fraud. The FCAS is a relatively new service, and the JMLIT has not made a public statement about its overall effectiveness to date. However, as an aspiration, and as the FCAS is refined in time, the hope is that the public sector can ultimately reap its benefits because giving the private sector access to updated threat alerts may generate more relevant and higher quality SARs.

Each of the aforementioned arrangements shares a notable feature: they are domestic. They involve national law enforcement agencies, regulators and domestic institutions (including the domestic operations of foreign-owned institutions), but are not available to participants located abroad. As financial crime threats become increasingly global, countries should consider how public–private platforms for sharing intelligence on money laundering and terrorist financing could become international in scope, drawing in foreign law enforcement operators and overseas financial institutions.

Regardless of the model adopted, governments should aim for the creation of public–private collaborative forums that foster trust among participants, improve the frequency and quality of information available, focus on high-priority threats, and involve the participation of the appropriate stakeholders required to tackle those threats.

**Enabling Private–Private Exchanges**

Improved public–private partnerships are only one piece of the puzzle. Ongoing exchanges of information within the private sector are also critical to improving FININT.

Private–private exchanges help to establish a culture of responsible information sharing among financial institutions. By putting financial institutions at the forefront of collaborative FININT generation, private sector-led initiatives can help to foster a sense among financial institutions that they have the public’s trust to act against sensitive threats. Furthermore, private sector-led arrangements allow financial institutions to be more than just ‘box tickers’ that file SARs; rather, they enable financial institutions to act as proactive generators of FININT. They also allow private sector participants to educate one another about emerging threats without having to rely too much on the public sector as an intermediary.

The best known private–private FININT initiative is Section 314(b) of the 2001 USA PATRIOT Act. Under Section 314(b), US financial institutions may share information about customers, accounts or transactions if they have concerns of money laundering or terrorism. By sharing

---


31. BBA, ‘Banks Team Up with Government to Combat Cyber Criminals and Fraudsters’.

these details, financial institutions can build a more complete picture of end-to-end financial activity than when they operate alone, leading to higher-quality SAR filings. The measure provides participating institutions with safe harbour from liability for the disclosure of personal data under certain conditions; for example, firms must register their intent to participate in the programme and they must maintain adequate data security practices. The initiative operates on the premise that the major obstacle to private–private information sharing on money laundering and terrorist financing is financial institutions’ concern about liability for customers’ data privacy. Private sector actors therefore require assurance that if they were to share information in a secure and responsible way, they will not face litigation.

Annecdtal accounts suggest that Section 314(b) facilitates enhanced SAR reporting among participants and fosters a more robust culture of information sharing within the US private sector since 9/11. However, the voluntary participation of the private sector in Section 314(b) has not been as widespread as policy-makers and regulators had hoped. This suggests that merely providing legislative frameworks and authorisation to share information is insufficient. Section 314(b) authorises information sharing but is not itself a platform for sharing in the manner of the JMLIT. The US also lacks widely available IT platforms or collaborative task force-type forums that can facilitate efficient and secure networking and communication among financial institutions. Governments considering the provision of similar authorities must therefore think carefully about how to ensure that the private sector has a broad mandate to share information, but with the support of effective collaborative platforms.

Despite its limitations, Section 314(b) offers the most polished model for ongoing private–private FININT sharing to date. At the time of publication, the UK is considering implementing safe harbour provisions similar to those set out in Section 314(b) to enable wider data sharing between firms, including under the auspices of the JMLIT. In May 2016, Singapore announced plans for a pilot programme to enable private–private sharing. While few details are publicly available, this arrangement would reportedly involve allowing the largest banks in Singapore – including, eventually, foreign banks with branches there – to share customer due diligence information. The aim is to allow banks to make informed decisions before establishing relationships with customers in order to mitigate exposure to financial crime risks.

Stakeholders concerned with enhancing FININT on money laundering and terrorist financing could also learn from anti-fraud and anti-cybercrime efforts. One industry-led fraud intelligence sharing model in the UK is Cifas, a non-profit company which facilitates UK private sector collaboration on fraud risks. Cifas maintains a national fraud database, which allows its approximately 300 members to access live information on member-submitted incidents of

33. Ibid.
34. Ibid., pp. 12–14.
35. Ibid., pp. 20–21.
38. Cifas originally stood for ‘Credit Industry Fraud Avoidance Service’.
confirmed fraud. Members can use this information to verify whether individuals they suspect of fraud have already been identified as fraudsters by other members. A bank processing a mortgage application, for example, could check the database to determine whether other firms have reported the individual as a fraudster – reducing the risk of a loss of funds by the querying bank. In a sign of industry confidence in the Cifas model, some respondents to a 2015 request from the Home Office and HM Treasury for views on enhancing the UK SAR regime suggested that the UK should have Cifas-like arrangements for money laundering and terrorist financing.

With respect to cybercrime, the US-based Financial Services Information Sharing and Analysis Center (FS-ISAC) acts as a global focal point for industry to share intelligence on cyber- and physical security threats. Established by US financial institutions in 1999, and owned by its member institutions as a non-profit company, FS-ISAC’s membership now includes more than 6,000 private sector participants from nearly 40 countries. Similar international networks for sharing intelligence on money laundering or terrorist financing would be welcome, even if such extensive global membership may not be realistic in the near term.

The prospect of private–private information sharing is likely to raise concerns about the consequences for the integrity of personal financial data. This is a legitimate concern and should not be minimised. If banks share information about customers, accounts and transactions, there is naturally a risk that information could be mishandled, lost or stolen in the process of its transfer. Furthermore, there is a risk that financial institutions could exchange information about individuals whom they wrongly suspect of involvement in illicit activity.

To address these concerns, private–private information sharing arrangements should include controls designed to safeguard customers’ sensitive data, such as:

- Criteria that financial institutions must meet before they share information. For example, under Section 314(b) of the USA PATRIOT Act, to prevent indiscriminate data transfers, participating institutions may only share information where they can demonstrate that the information is being used to: report on money laundering or terrorist financing; determine whether to facilitate business; or assist in otherwise meeting AML/CTF requirements.
- Obligations on financial institutions to document policies and procedures for securing customer information.
- Obligations on financial institutions to demonstrate that they have the necessary IT arrangements for safely transferring customer data.
- Requirements that financial institutions anonymise certain types of information, such as sensitive data identifying a customer or account details.

• Fines and other penalties for firms that fail to meet data protection standards or that engage in negligent and wilful sharing of non-pertinent information.

If robust customer data protection controls such as these exist, along with safeguards to protect financial institutions against liability, private-private exchanges can result in enhanced FININT generation conducted in a responsible manner.

**Expanding Official Collaboration**

Ultimately, in order to counter illicit financial activity globally and to disrupt cross-border threats, governments must be able to share FININT with one another. At the May 2016 international Anti-Corruption Summit in London, participants agreed to ‘expand sharing initiatives by allowing FIUs to exchange information spontaneously’ in order to combat corruption.43

A number of important mechanisms for public sector collaboration exist. Many countries have established bilateral agreements that permit their FIUs to exchange information. For its members, the Egmont Group acts as the international focal point through which they may exchange information and communicate. The Egmont Group also establishes international standards and operating rules for conducting information exchanges between countries. Furthermore, it acts as a gateway through which countries’ public and private stakeholders can indirectly obtain information from other countries about financial crime threats.44

Despite these important arrangements, both within and outside the Egmont Group more frequent exchanges of information could occur, and the quality of exchanges could be more robust. A current disadvantage is that the heavy reliance on bilateral exchanges at times limits the ability to act effectively against illicit finance networks operating across numerous jurisdictions.45 To improve this situation, partner countries should endeavour to permit and undertake multilateral information exchanges as widely as possible.

Some countries have recognised this need. In Europe, countries benefit from a decentralised network, FIU.net, which facilitates multilateral co-operation among EU FIUs (Chapter 3 of this Occasional Paper examines this platform more closely). As another example, in November 2015, Australia and Indonesia hosted the first Southeast Asian regional summit on counter-terrorism financing, bringing together representatives from nineteen countries to commit to establishing regional CTF solutions. Participating countries agreed to form a task force to develop regional, multilateral information sharing approaches.46 While only in its formative stages, this Southeast Asian initiative offers a promising experiment in region-wide co-operation and possibly also a template for other regions.

The Egmont Group has an important role to play in facilitating these exchanges. It offers the expansive networking platform required for undertaking multilateral co-operation and can also assist by sponsoring more frequent, collaborative studies of key threats. For example, the Egmont Group sponsored a study in 2015 of the financing methods used by Daesh (also known as the Islamic State of Iraq and Syria, ISIS) that drew on intelligence provided by 40 members about terrorist fighters travelling to Iraq and Syria. This information allowed FIUs to map terrorist networks and share information with the private sector on terrorist financing threats and trends. Additional collaborative exchanges of this variety should be an international priority.

Extending official collaboration in such ways may well prompt concern that FIU exchanges could result in the transfer of personal information to foreign governments, particularly those with undemocratic practices and non-transparent judicial systems. Such concerns are understandable, but established standards framing exchanges between international FIUs reduce such risks. When FIUs use the Egmont platform to exchange information on subjects of interest, they do not engage in data mining or other indiscriminate use of bulk information. Rather, FIUs exchange information on the subjects of law enforcement and regulatory investigations, making it unlikely that information about someone who is not already a suspect would be exchanged through such channels. FIUs are also able to exercise discretion about the types of information they choose to share and with whom. Furthermore, as Chapter 3 of this paper will show, new IT developments are enabling FIUs to share information in ways that are increasingly secure.

Multilateral FIU exchanges offer just one prospect for enhanced official collaboration. Another approach is to supplement FIU exchanges with more frequent FININT exchanges outside the FIU context. While FIU exchanges are essential and beneficial, capacity constraints, technological limitations, outdated legal frameworks and the absence of mechanisms for sharing information may at times hinder them. Governments may therefore benefit from integrating FININT exchanges into other existing information sharing mechanisms that do not involve FIUs. For example, the US has enhanced its information sharing capabilities by integrating its FININT collection efforts into the broader efforts of the US Intelligence Community. In 2003, Congress authorised the establishment of the Department of the Treasury’s Office of Intelligence and Analysis (OIA), which acts as the Treasury’s intelligence analysis arm and establishes national FININT collection priorities. This allows the Treasury to obtain FININT through the Intelligence Community’s wide variety of classified and open source intelligence gathering methods. The OIA’s mandate includes pursuing the downgrading and declassification of intelligence to enable the sharing of specific risks with foreign governments, as well as domestic and foreign financial institutions. This willingness to operate outside of an FIU context enables the US to play a proactive, leading role in sharing FININT internationally.

47. Ellis and de Oliveira, ‘Tackling Money Laundering’, p. 27.
50. Ibid., pp. 9–10.
II. Navigating SAR Confidentiality

THE FATF RECOMMENDATIONS, the international standard by which countries establish domestic AML/CTF frameworks, have long emphasised the importance of SAR confidentiality. In Recommendation 21, the FATF indicates that countries should construct their legal frameworks so that:

Financial institutions, their directors, officers and employees should be:

(a) protected by law from criminal and civil liability for breach of any restriction on disclosure of information ... and ...

(b) prohibited by law from disclosing (“tipping-off”) the fact that a [SAR] or related information is being filed with the FIU.¹

The premise is simple: financial institutions should not be constrained by contractual or other obligations from filing a SAR that could provide law enforcement agencies with information about potentially illicit activity; but the integrity of that information is also reliant on its confidentiality. Customers, members of staff not directly involved or third parties (such as other financial institutions) should not learn that a SAR was filed in case that disclosure would jeopardise an investigation and reveal the identity of the submitter.

In practice, however, approaches to date on SAR confidentiality present certain challenges for generating FININT. When financial institutions are unable to share SARs, or even discuss a SAR filing, with their foreign branches and affiliates, it creates the risk of the company being party to illicit financial activity involving its customers.

Similarly, because financial institutions cannot inform an FIU in one country that they have filed a SAR with another country’s FIU, law enforcement agencies must connect the dots about any shared interest in cross-border targets. This creates significant inefficiencies in co-ordination. Furthermore, the question about what constitutes ‘tipping off’ can prove confusing to many in the private sector and can inhibit information sharing.

This section surveys the ways in which SAR confidentiality practices inhibit information sharing, and it considers how policy-makers might surmount those challenges.

Enterprise-Wide Sharing

Increasingly, financial enterprises with numerous branches or affiliates, whether operating in one country or many, pursue group-wide AML/CTF risk management. There is good reason to do so. For example, a UK banking group with numerous domestic and international branches may struggle to identify risks across its enterprise structure if each branch has a separate approach to risk detection and risk management. Thus, the group’s head office should establish global policies and procedures that set minimum standards across the group to ensure the harmonisation of efforts. However, if a customer has an account at multiple branches of the banking group in numerous jurisdictions, but those branches are unable to share information with one another about that customer’s suspicious behaviour, there is a risk that illicit financial activity might go undetected across part or all of the group. Conversely, with permission to share SARs and related data across their international networks, financial institutions are better equipped to detect and report suspicious activity. As the Egmont Group summarises the issue:

The ability to share information on suspicious transactions across the financial group should enhance all aspects of compliance, including ... suspicious transaction reporting. Financial groups should be able to incorporate a wider, enterprise-wide view of the activities of the [SAR] subjects, thus giving FIUs more valuable information.2

Even if the benefits of enterprise-wide sharing seem obvious, it is important not to dismiss the implications of SAR confidentiality requirements; indeed, standards of confidentiality remain essential. If a bank shares a SAR – or even discloses the fact of a SAR filing – with a member of its wider banking group, this creates the risk of ‘tipping off’. Once the original branch shared that it had filed the SAR, the mere fact that it had filed a report with the FIU could potentially get back to the customer. This risk is particularly high if a bank were to share its SAR information with an affiliate branch in a country with poor AML/CTF standards. For example, US or EU banks might be reluctant to share SAR information with affiliated branches in parts of Africa, Asia or the Middle East.

Similarly, not all foreign jurisdictions recognise the confidentiality of other countries’ SARs.3 If a foreign legal system allows for discovery of another country’s SARs and requires their presentation as evidence during legal proceedings, it could compromise the source of that information. It could also compromise the home countries’ law enforcement investigations. Furthermore, because SARs only indicate suspicions of illicit behaviour, rather than representing proof upheld to a criminal standard, there is a risk that individuals’ private financial information could be jeopardised based on mere suspicion. Furthermore, there is a risk that those named in SARs might become victims of ‘financial exclusion’ or might be denied access to financial services if a wide range of financial institutions were to become aware of the reports.4

3. Ibid., p. 16.
obligations, the integrity of the sensitive information they disclose to FIUs, and the effectiveness and security of investigations into suspected illicit activity.

Despite these risks, there are a number of vocal proponents of increased enterprise-wide information sharing, including prominent financial institutions. For example, The Clearing House, which acts as an association of the largest global commercial banks, has led the argument for permitting US financial institutions to share SARs across their international enterprises. The US FIU, the Financial Crimes Enforcement Network (FinCEN), has previously clarified that certain US financial institutions may share SARs with their US affiliates that are also subject to US SAR requirements.5 US branches of a foreign bank may also share SARs with their non-US parent. This latter provision permits the parent entity or head office to undertake enterprise-wide monitoring of financial crime risks.6 However, US-domiciled financial institutions are still unable to share SARs, and disclose the fact of a SAR filing, with their foreign branches or subsidiaries.

The Clearing House maintains that this barrier significantly hinders US financial institutions’ ability to conduct enterprise-wide risk management. The Clearing House has therefore called on FinCEN to permit US financial institutions to share SARs with their foreign branches and affiliates provided they meet several conditions. For example, FinCEN could permit US institutions to share SARs only with foreign branches based in FATF member countries. If a foreign branch is based in a non-FATF member country, The Clearing House suggests that the US institution and its foreign partners should enter into a confidentiality agreement governing the terms of exchange.7

These recommendations do not address every concern about enterprise-wide SAR sharing. They do, however, suggest that greater enterprise-wide sharing is achievable when countries are intent on establishing clear guidelines. For example, countries might require firms to have clear, written policies and procedures for overseas SAR transfers. Enterprise-wide sharing arrangements should also include requirements that firms prioritise the safeguarding of customer data. For instance, firms should only be permitted to share information among individuals who have a genuine ‘need to know’; and should be able to demonstrate that they have appropriate arrangements in place for transferring SAR information securely (by for example, using encrypted e-mail or secure internal data retention systems). If the prospect of enterprise-wide sharing with all affiliates is too broad for comfort, countries might adopt their own lists of equivalent jurisdictions with acceptable standards. France, for example, permits financial institutions to share with foreign group members the fact and substance of SARs filed with the French FIU, Tracfin. However, such sharing may only occur with group entities in

approved countries with equivalent AML/CTF standards (such as the US and other EU countries) and adequate data protection frameworks.\(^8\)

FinCEN has responded cautiously to US banks’ requests for greater enterprise-wide sharing. Although it has left open the possibility of permitting US banks to share information with foreign branches, FinCEN has expressed significant concerns that foreign jurisdictions do not ensure the confidentiality of US SARs in their court proceedings.\(^9\) Such concerns are valid, as the US legitimately fears that more permissive SAR sharing could undermine the integrity of its domestic SAR regime, which remains the critical source of domestic FININT. Furthermore, securing guarantees for US SARs to remain confidential in foreign courts would likely prove to be complex and time consuming.

Other countries, however, do permit relatively generous enterprise-wide sharing, which suggests that progress on navigating SAR confidentiality requirements is achievable with time. In the EU, Article 28 of the Third Money Laundering Directive offers member states a basis for enterprise-wide sharing.\(^10\) France has used this as the basis for its SAR-sharing model.\(^11\) Australia has similarly permitted enterprise-wide SAR sharing between Australian financial institutions and certain members of their business groups abroad.\(^12\) At least one financial institution in Australia has suggested extending these provisions to permit sharing with an even broader range of non-domestic group affiliates.\(^13\)

A multitude of approaches is possible. In lieu of near-term arrangements that will ensure global harmonisation of practice, the Egmont Group has suggested that countries aim to achieve bilateral or multilateral agreements to align their legal approaches and treatment of SAR confidentiality where possible.\(^14\) Where significant barriers or concerns continue to exist (as in the case of the US), partner countries should make high-level, joint political commitments to explore ways to identify and address the legal barriers to greater information sharing, while maintaining the integrity of sensitive data.

---


\(^11\) Ibid., p. 32.

\(^12\) Ibid., p. 34.


Most importantly, financial institutions should have greater ability within reasonable limits to notify foreign partners of SAR filings and share related information leading to higher-quality FININT across the company.

**Cross-Border FIU Notifications**

At the UN’s April 2016 summit on CTF, some public and private sector participants cited a particular barrier to information sharing: the inability of a financial institution to disclose to an FIU in one country that they have filed a SAR with an FIU in another.15

As an example, Duncan DeVille, Western Union’s global head of financial crime compliance, noted that Western Union received 75 subpoenas from law enforcement agencies in six different countries after the November 2015 attacks in Paris. This led Western Union to uncover information on more than 850 suspected individuals. Western Union had obligations to file SARs on these subjects in multiple jurisdictions; this created a complex web of reporting obligations due to the number of requesting countries.16

Although this caused an administrative challenge for Western Union, it was also inefficient for law enforcement. If Western Union could inform each respective government’s FIU that it had filed SARs with the other FIUs on those same subjects, law enforcement agencies would not have to spend time determining whether common investigative interests existed.

As noted earlier, collaborative networks such as the Egmont Group help FIUs to establish connections about investigative subjects of interest. Under current international sharing arrangements, however, there is a risk that governments might fail to make a connection about targets of mutual interest in a timely manner, or might miss them altogether. However, if a firm with branches in two or more countries could notify respective FIUs of their SAR filings, law enforcement agencies could make connections that are more straightforward and in a more timely manner.

As with enterprise-wide sharing, cross-border FIU notifications would naturally raise concerns, particularly about the risk of jeopardising ongoing law enforcement investigations. However, partner countries could enter bilateral or multilateral agreements to facilitate and govern cross-border FIU notification. Governments could also limit the scope of sharing by only permitting firms to inform another FIU that they have filed a SAR in the home country on a particular individual or entity, possibly using a unique SAR reference number, without permitting disclosure of the actual details of the SAR. This would assist FIUs in making common

---

15. Duncan DeVille, speech given during a UN joint open briefing of the Counter-Terrorism Committee and the 1267/1989/2253 ISIL (Da’esh) and Al-Qaida Sanctions Committee, ‘Countering the Financing of Terrorism and Depriving Terrorist Groups, Particularly Al-Qaida, ISIL (Da’esh) and their Affiliates, from Their Sources of Funding’, New York, 14 April 2016.

connections without jeopardising underlying sensitive information. Governments might also strictly limit the list of countries to which they would permit such notifications, and could even limit such notifications to specified, more serious risks or instances where a firm produced a SAR in response to a production order or subpoena.

In addition to prohibiting financial institutions from notifying other FIUs of SAR filings in the home country, most jurisdictions do not permit their financial institutions to file SARs directly with other countries’ FIUs. For example, if a bank has branches in three different countries and has suspicions related to a transaction that passed through all three countries, it is likely that all three branches would have to file separate SARs with their respective FIUs directly – often faced with the barriers to enterprise-wide sharing discussed earlier in this chapter. However, as a former director of FinCEN has noted, ‘it would be much more practical, timely, and ultimately effective’ if the head office could file a report directly with each of the FIUs in jurisdictions where it suspects illicit activity may be taking place.

The current ‘territoriality’ of SAR regimes is therefore an impediment to rapid and effective information sharing. Technological innovations – such as FIU.net – offer some hope for remediating these inefficiencies. Where regional FIU networks have established bilateral relationships, IT innovations offer the prospect of further enabling cross-border SAR reporting – that is, enabling a financial institution in one country to file a SAR directly with another country’s FIU. However, even with these IT innovations, changes to regulatory and legislative frameworks would be necessary to permit freer exchanges and cross-border SAR filings on a wide international basis.

**Clarifying ‘Tipping Off’**

Merely permitting greater enterprise-wide sharing or cross-border FIU notifications may not be enough to ease firms’ concerns that they could be held liable for inappropriate disclosures. Even with permission to disclose SAR filings more widely, firms will require assurance that doing so will not make them accountable for committing a tipping off crime.

To this end, governments may need to reconsider the appropriate scope of tipping off offences while upholding the core principle of confidentiality. This may require, in some instances, clarifying that firms will not be accountable should a third party leak the information in violation of confidentiality agreements. As part of an ongoing review aimed at enhancing the UK’s SARs regime, for example, the Home Office and HM Treasury have received feedback from the private

---

17. According to the Egmont Group’s 2008 survey, only 8 per cent of jurisdictions surveyed permitted their financial institutions to file SARs directly with foreign FIUs. Egmont Group of Financial Intelligence Units, ‘Enterprise-Wide STR Sharing’, p. 18.


19. The Egmont Group describes the ‘territoriality’ of SARs as the expectation that banks in any given jurisdiction must report SARs only to their domestic FIU. Egmont Group of Financial Intelligence Units, ‘Enterprise-Wide STR Sharing’, p. 41.

20. Author’s discussions with FIU experts, June 2016.
sector that the UK’s tipping off provisions are not fit for purpose. Other countries should undertake similar reviews to determine whether their tipping off provisions inhibit information sharing. The FATF in particular can play an important role in providing guidance to countries on how best to manage this challenge.

III. Harnessing Technology

TECHNOLOGICAL INNOVATION OFFERS a promising solution to a number of the information sharing challenges discussed above. Appropriate technological solutions can enable more rapid exchanges, expand the prospect of multilateral sharing and help to ensure the integrity of sensitive customer data or SAR information.

To improve the capability of information sharing arrangements, governments are exploring IT platforms that permit greater cross-border collaboration. Collections of financial institutions and IT developers are also exploring solutions to enhance private–private collaboration.

This section examines a number of ongoing efforts to harness technology and considers several key issues in their development.

Integrating and Embedding Systems

The history of established information sharing programmes offers instructive lessons about the importance of technology for the effectiveness of FININT exchanges.

In the case of Section 314(b) of the 2001 USA PATRIOT Act, private sector participation suffers from the lack of platforms. The government has left the private sector largely to its own devices to determine how to identify other programme participants and actually transfer sensitive data. Consequently, many US financial institutions are reluctant to collaborate given their concerns about remaining compliant with requirements to protect information.¹

At the international level, the Egmont Group provides an IT platform, the Egmont Secure Web (ESW) system,² which allows more than 150 member countries to make and respond to bilateral requests regarding specific investigative targets using encrypted e-mail.³ However, the ESW is not a sophisticated platform, and Egmont is working to enable more fluid information sharing as well as to enable multilateral exchanges via the system.⁴

Since the establishment of the above programmes and platforms, technological innovation has broadened the potential for information sharing. New platforms offer the prospect of more rapid and efficient information sharing among a larger number of stakeholders, while ensuring the security of sensitive information. In particular, FININT sharing is already benefiting from the concept of ‘privacy by design’ – the notion that data security should be integral to the

---

2. The ESW platform is formally hosted and administered by FinCEN in the US.
design of IT platforms and that sensitive data should be transferred and retained under specific conditions and for specific purposes only.\(^5\)

An example of privacy by design is the embedded Ma³tch technology – with ‘a³’ referring to ‘autonomous, anonymous, analysis’ – used by FIU.net.\(^6\) Launched as a pilot programme in 2004,\(^7\) and made formally operational in 2007,\(^8\) FIU.net initially functioned as an online network for member state FIUs to create linked cases about suspects on which they could collaborate. FIU.net integrated the Ma³tch solution into its operations in 2012, significantly enhancing the platform’s intelligence capabilities.\(^9\) Ma³tch enables all 28 EU member states to engage in secure networking by allowing member state FIUs to survey FIU.net and determine whether other FIUs have an interest in a subject of investigation.\(^10\) Ma³tch uses encryption methods to secure personally identifiable information (PII):\(^11\) when an FIU queries the system with the PII of a subject of interest, Ma³tch encrypts that information and relies on algorithms to match it with other FIUs’ inputs on the same subject; once FIUs make a connection, they can make contact and begin sharing information. Importantly, information exchanges between countries can only occur after Ma³tch has identified that a common investigative interest exists between FIUs. PII does not leave the querying country’s home databases when it makes the query, and the owner of the information is able to control any further exchange once they have identified a shared investigative interest with another FIU.\(^12\)

Prior to the use of Ma³tch, information sharing between European FIUs was less efficient: if an EU FIU wished to determine whether a peer FIU had information on a subject of interest, it used the ESW, which primarily facilitates bilateral information sharing. FIU.net, on the other hand, offers a platform for multilateral information sharing, and Ma³tch technology ensures that this information sharing is secure and compliant with EU data privacy requirements by encrypting PII at the initial point of contact. A distinct advantage of the current platform is that information sharing among participants is pertinent: the exchange of information only occurs after FIUs have discovered a common interest. This makes FIU networking both more secure and more efficient.

---

7. Ibid.
11. PII refers to any data that could be used to identify a specific individual, such as date of birth, tax identification number or passport number.
Another advantage of FIU.net is that it operates as a decentralised network. One option for establishing information sharing platforms is to store data centrally, where all members may have simultaneous access to data. Centralised data storage, however, makes it more difficult for individual members to ensure the integrity of data for which they are responsible. With FIU.net, however, each member state FIU maintains its own database for PII and other sensitive data. These local databases are compatible with the FIU.net platform, but this data never leaves the member state’s home database – Ma3tch ensures that data remains stored with its owner throughout the networking process. This also permits clear lines of responsibility: member state FIUs remain responsible for the handling of data, for updating information that flows through the network and for ensuring that the information provided is accurate.

Anecdotal information suggests that FIU.net participants find the platform user friendly and efficient. One advantage is Ma3tch’s ‘autonomous’ function, which allows users to choose from its variety of search tools and data generation capabilities. This is critical in the EU, where member states have vastly different resources and the domestic databases that interface with FIU.net are of vastly different levels of maturity. Ma3tch therefore enhances collaboration while avoiding a one-size-fits-all approach.

In the US, a number of financial institutions and IT companies have begun to develop solutions for facilitating private sector exchanges under Section 314(b) of the PATRIOT Act. These solutions operate under ‘privacy by design’ principles similar to those of FIU.net: they ensure that financial institutions retain control over their data while significantly streamlining the networking process which allows them more quickly to identify peers with pertinent interests. These solutions are not yet widespread. Anecdotal discussions with experts also support the view that some private sector IT platforms are still in early stages of maturity and are not always user friendly. Even so, private sector-driven solutions offer hope that information sharing could become more widespread in the US financial sector.

Industry participants are also looking to innovations such as blockchain technology to improve information sharing. Blockchain is a ‘distributed ledger technology’ originally developed as a publicly available record-keeping system for the cryptocurrency Bitcoin. Put simply, blockchain is an efficient means of consolidating information from decentralised networks, offering the

13. Ibid.
15. Author’s discussions with experts, May 2016.
17. Author’s discussions with financial crime compliance and IT experts, February 2016.
Making Information Flow

prospect of more efficient and transparent data retention and access. Trade finance institutions, for example, are exploring the use of blockchain to share information with private sector peers to prevent losses from invoice fraud.\(^\text{19}\) Blockchain also offers a potential solution for international financial groups to engage in more efficient enterprise-wide information sharing across corporate networks.\(^\text{20}\) However, blockchain is still in the early developmental stages, and its ultimate prospects as a comprehensive solution to information sharing remain unclear.\(^\text{21}\)

A key lesson here is that the integration of appropriate IT solutions should be a priority when establishing information sharing arrangements. Of course, some degree of catch-up is inevitable where information sharing programmes already exist and use legacy systems – as is some degree of retrofitting new solutions to old arrangements. FIU.net, for example, has become valuable because it harnesses up-to-date IT solutions and makes technology central to its operations.

The Egmont Group has recognised the need to harness technology to enable more robust multilateral exchanges of information. Egmont has drawn on FIU.net as a model for expanding its own information sharing platforms, particularly in countering terrorist financing.\(^\text{22}\) Egmont’s Information Technology Working Group will have an important role in advancing the discussion about multilateral sharing.\(^\text{23}\) A key question at the international level is where the storage, maintenance and governance of more advanced systems should rest. While a decentralised platform has functioned well in the context of the EU, it may prove politically and practically challenging across the vast membership of the Egmont Group.

**Funding**

The funding of IT platforms is of course a critical consideration. Information sharing arrangements should include adequate funding to develop and integrate fit-for-purpose IT platforms. In the case of FIU.net, participating members have provided funds for the system, which until 2015 also received funding from the European Commission.\(^\text{24}\) In the case of Egmont, membership dues

---


fund operations such as the ESW. The UK Home Office has suggested that all parties that benefit from the UK’s IT systems for SARs should contribute to funding upgrades to the systems; this would presumably include both public and private sector stakeholders. For IT solutions intended to enable private–private information sharing, funding might take a number of potential forms: public sector funding of private innovations; joint public–private sector funding; or purely private sector financing. A priority for future official exchanges should be ensuring sufficient funding specifically for developing and embedding IT platforms from the outset.

IT innovations, however, are not a cure-all. The balance between fluid information sharing and data security will remain a delicate one. Technological development requires governing principles that guarantee its use in a manner consistent with broader policy aims and the public interest. It also requires appropriate legal frameworks at the national and multilateral levels to ensure accountability. Systems will always remain vulnerable to human error and abuse; therefore, robust quality assurance and audit arrangements must be in place to ensure that users operate systems in accordance with their intended purpose. Ultimately, the success of AML/CTF efforts relies on the skill, expertise and effort of individuals who represent the public and private sectors.

IV. Summary and Conclusions

INTERNATIONAL EXPERTS IN financial crime increasingly recognise that greater FININT sharing is a critical global security priority. Acknowledging the nature of the problem is only a first step. To have an impact on evolving security threats, policy-makers must implement concrete measures that enable more frequent and meaningful information sharing.

Making information flow is, and will remain, a tremendous challenge. Data protection concerns, inconsistent legal frameworks and antiquated systems are only a few of the many barriers that inhibit more robust, global exchanges of information on money laundering and terrorist financing. For example, customers of financial institutions rightly worry about the safety of their personal data as public and private sector stakeholders carry out exchanges; and financial institutions for their part are often reluctant to share information for fear of liability for mishandling sensitive data. Furthermore, from country to country, laws differ significantly regarding the protection of customer data and the ability of firms to share SARs. In turn, these jurisdictional legal discrepancies inhibit the ability of the public and private sectors to identify and tackle cross-border threats. Even where public and private sector stakeholders have a clear mandate to share information, outdated IT platforms hinder information sharing, slowing it down and making it less efficient, as well as increasing the risk of sensitive data being compromised.

Nonetheless, there are practical solutions that countries can begin to implement to facilitate more expansive FININT exchanges.

Broadening and deepening networks is essential for ensuring that all necessary stakeholders have access to information to allow them to play a meaningful role in identifying and disrupting threats. In particular, stakeholders must endeavour to improve and expand collaboration in three realms: between the public and private sectors; within the private sector; and between countries.

A number of potential solutions exist: public–private task forces targeting high-priority threats; industry-driven collaborative intelligence sharing; and regional, multilateral FININT exchange initiatives. Whichever models governments, financial institutions and international organisations adopt, the aim should be for these mechanisms to target high-priority security concerns in an efficient fashion.

Countries must also find practical ways to navigate the challenge of SAR confidentiality more effectively. This does not mean abandoning confidentiality as a key principle of the global AML/CTF regime. However, limits on international enterprise-wide SAR sharing constrain the private sector from successfully identifying and managing money laundering and terrorist financing risks. Similarly, global law enforcement efforts would be more efficient if financial institutions could make cross-border notifications of SAR filings to foreign FIUs. Such measures will require precise standards and safeguards, including carefully designed safeguards to ensure
the integrity of customer data; and countries may need to update legislative frameworks to clarify that the sharing of SAR information by the private sector with appropriate parties will not constitute tipping off when done securely and in good faith.

Finally, stakeholders in the public and private sectors can address concerns about the transmission of sensitive information in part by harnessing technology. Innovations are enabling public and private sector stakeholders to network more efficiently while ensuring that data remains secure. Some early attempts to implement information sharing programmes have suffered at times because they lacked effective IT platforms as a feature of their design. Future information sharing arrangements should therefore include the integration of IT platforms as a central element. This will require sustained engagement and funding from both the public and private sectors. To ensure information sharing arrangements remain consistent with data privacy requirements, stakeholders must commit to developing IT solutions that ensure the integrity of sensitive information, provide for accountability and are subject to rigorous oversight. IT solutions must not, however, be seen as a substitute for the adequate funding of skilled human resource. Individuals’ competence and expertise will remain essential.

While daunting, increasing the flow of financial information is achievable. Indeed, as this Occasional Paper has shown, a number of countries have begun to do just that. As these efforts evolve, stakeholders should broaden their scope and membership to ensure that the international community can address global threats comprehensively.

To achieve these aims, policy-makers should consider the recommendations set out in this paper’s Executive Summary.
About the Author

David Carlisle is an independent consultant specialising in devising strategies for combating financial crime. He has worked in London since 2012. From 2007 to 2011, David held various roles in the US Department of the Treasury’s Office of Terrorism and Financial Intelligence, where he worked on US policy related to anti-money laundering, countering terrorist financing and economic sanctions regimes. David holds a Masters in International Relations from the Johns Hopkins School of Advanced International Studies.