Occasional Paper

Tackling Money Laundering
Towards a New Model for Information Sharing

Clare Ellis and Inês Sofia de Oliveira
Tackling Money Laundering
Towards a New Model for Information Sharing

Clare Ellis and Inês Sofia de Oliveira

Occasional Paper, September 2015

Royal United Services Institute
for Defence and Security Studies
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 2015 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/>.

Printed in the UK by Stephen Austin and Sons, Ltd.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)
Executive Summary

On 26 and 27 May 2015, RUSI welcomed over seventy participants from Europe, North America and Australasia to a discussion on ‘Tackling Money Laundering: Towards a New Model for Information Sharing’. This two-day conference, hosted by RUSI’s Centre for Financial Crime and Security Studies, brought together national financial-intelligence units (FIUs), law-enforcement officials, prosecutors and senior figures from the financial-services industry. The principal aim was to promote partnership-oriented, innovative and targeted strategies to enhance current practices and develop a new model for information exchange. Participants focused on the challenges associated with sharing information in complex, multi-jurisdictional money-laundering investigations.

Information sharing was seen as a fundamental tool for effectively tackling illicit financial flows; however, it was equally agreed that current governance models require additional debate and improvement. Specifically, the following issues were identified:

- Across the various represented sectors and jurisdictions it was recognised that financial intelligence (FININT) is underused. Limited public-sector resources – both staff and infrastructure – contribute to this failing and foster frustration within private partners whose investments in detecting illicit activity are not always followed by investigations.
- Once the private sector identifies and reports suspicious financial activity, data-protection regulations and restrictions surrounding the content of their reports also represent a critical obstacle to information sharing. Restrictions on the ability of the private sector to share information, within jurisdictions and across borders, reduce the quality and comprehensiveness of their suspicious transaction reports, increasing the investigative burden on law enforcement.
- Between public bodies, co-operation at the national level is sub-optimal, while international information exchange is lengthy and cumbersome, meaning that information is rarely received in time to contribute to an active investigation.

The ultimate result of these barriers is limited impact and poor efficiency in the fight against illicit finance. The resources and intelligence available within the private sector, within public bodies and across jurisdictions are rarely used to maximum effect.

Based on the conference discussions, we advocate the establishment of a new model for information sharing that is guided by the principle of effectiveness and based on three pillars: a clear legal framework; improved resourcing; and facilitated co-operation between public and private sectors and internationally. Specific recommendations under these pillars are outlined below.
Effectiveness

An overarching theme across these pillars is the use of FININT. Governments must learn to set priorities and communicate them to the private sector in order to ensure better quality reporting and contribute to the joint improvement of the legal framework. This would create a virtuous circle of increased effectiveness, as more appropriate strategies for disruption and prevention are developed, and more productive dialogue fostered with different stakeholders.

With the support of the research community, governments and law enforcement should therefore actively work with the private sector to:

1. Generate evidence-based research to further develop the concept and operational use of FININT.

Pillar One: A Clear Legal Framework

Revised data-protection provisions, or more effective guidance on the interpretation of current laws, will play a crucial role in improving the information-sharing system.

Data-protection laws must, at all stages, be accompanied by a sense of accountability. Governments and the private sector alike must offer reassurance by being publicly responsible – for example with regard to individual privacy – for the gathering, processing and updating of collected data for the purposes of combating financial crime. As we evolve into an increasingly international system, any future system must incorporate global standards. A comprehensive, standardised and clear set of data-protection provisions is therefore much needed.

To this end, governments should consider two measures:

2. Promote and disseminate information and guidance that clarifies data-protection requirements in the context of fighting financial crime
3. Request that the Financial Action Task Force (FATF) revisit its recommendations on reporting, FIUs and tipping-off in order to provide mechanisms for information sharing within the private sector. The FATF also needs to take a more active role in emphasising the importance of information sharing, perhaps including an assessment of this activity in its mutual evaluations.

Pillar Two: Improved Resourcing

The conference proceedings emphasised the need to provide the public sector with adequate resources, while simultaneously allowing the private sector to expand its information-sharing capabilities. Increased feedback and dialogue from the public sector, alongside the ability to co-operate and share information with other private institutions, would enable the regulated sector to provide better quality, more comprehensive and targeted information. Increased resources within the public sector would therefore have a force-multiplier effect on the overall
effort, enabling public bodies to capitalise on the significant investigative power and capability of the regulated sector.

Innovative technology-based resources will also be crucial in facilitating a new information-sharing model. FIU.Net – a decentralised, multinational network formed of several national FIUs which is designed to enhance information exchange among participating European countries – is a useful example. Conference conclusions suggest that further analysis is needed into the use of ‘privacy-by-design’ tools like FIU.Net’s Ma³tch that could be developed and expanded beyond the EU. The adoption of systems that facilitate efficient information sharing while simultaneously protecting individual rights would be an important first step towards developing a new model.

To support this pillar, governments should commit to four key measures:

4. Provide regulators and law enforcement with sufficient tools, resources and updated technology to operate effectively and fulfil their guidance role
5. Create regional bodies to facilitate information sharing across jurisdictions, using the FIU.Net model. These bodies should also be empowered to promote co-operation across groups and intra-group jurisdictions, forming a strong international network
6. Develop Ma³tch or similar privacy-by-design software for global adoption by each of these regional FIU.Net bodies to support both their individual roles and their co-operation
7. Partner with the private sector to enhance the availability of resources (for example through funding) to support information sharing.

Pillar Three: Facilitated Co-operation

Finally, improving and increasing co-operation between all participating actors and, particularly, jurisdictions will be paramount. Governments and the private sector should invest in a partnership approach that builds on permanent dialogue and exchange of information. Future efforts should focus on providing frameworks for dialogue and encouraging organisations such as the Egmont and Wolfsberg Groups – co-operative bodies consisting of FIUs and major banks respectively – to assume a greater leadership role for the public and private sectors respectively.

To achieve this, governments and the private sector should work together to:

8. Hold Wolfsberg Group-like bodies responsible for providing guidance to their members and establishing co-operation mechanisms that permit safe and effective data sharing. In essence, such organisations would reach beyond current membership and build towards a private-sector ‘Egmont’ function
9. Establish further initiatives based on the UK’s Joint Money Laundering Intelligence Taskforce model, increasing the platforms for dialogue between the public and private sectors
10. Support policy-making at FATF and national levels that is based on prevention and specific disruption objectives to avoid overburdening the system with defensive reporting and lengthy investigative practices.
Finally, governments should:

11. Increase the Egmont Group’s role as a pillar of international co-operation, in the context of information sharing, and revise national strategies for communication between public bodies.

Implementing these recommendations would increase effectiveness in the global fight against financial crime and represent significant strides towards a new model of information sharing based on public–private co-operation.
Introduction

The ability to share information is a fundamental characteristic of modern international relations and globalised commerce. In the context of the fight against financial crime, sharing information allows actors from different institutions, sectors and jurisdictions to exchange content that can assist in preventing crime, disrupting criminal activity and identifying the networks of perpetrators.

Money laundering, terrorist financing and wider financial crime are cross-border activities that know no geographical boundaries nor hold any respect for state limits. Solutions must therefore be sought at the national and international levels, and stakeholders from each relevant sector must come together to identify, clarify and jointly address the specific obstacles that hinder effective collaboration.

To facilitate this process, on 26 and 27 May 2015 RUSI hosted a conference entitled ‘Tackling Money Laundering: Towards a New Model for Information Sharing’. The event brought together members of the private sector, policy-makers, law-enforcement, prosecutors and academics for focused discussions on current information-sharing provisions, challenges and opportunities. Representatives from the public and private sectors, including law enforcement, financial institutions and prosecutors, from the UK, the US, Canada, South Africa, Australia, New Zealand, Spain, Belgium and the Netherlands were in attendance and participated in the discussion.

This occasional paper reflects on these proceedings and provides a detailed analysis of the major obstacles to more efficient information sharing. It draws on the insights provided at the conference to suggest measures which could encourage a more effective exchange of information between private and public actors, both domestically and internationally.

The conference highlighted a significant willingness to co-operate among the different parties and across jurisdictions. Attendees repeatedly stressed the existence of common ground and consequently a strong foundation on which change and reform can be built – if provided with the right amount of public and private commitment.

It was acknowledged that active participation of national and international legislatures in reviewing current frameworks is vital for lasting, substantial change, given that information sharing encompasses political, legal and international policy challenges. Newer and more efficient software alternatives to information-sharing management were suggested as possible solutions to the identified IT and data-processing inefficiencies. Opportunities for dialogue and co-ordination also emerged as a key concern linked to the lack of resources and poor responsiveness of international co-operation efforts.
There was unanimous agreement that an effective information-sharing model is critical in tackling financial crime. Greater co-ordination among actors, adequately resourced public bodies and increased international co-operation would help to develop such a model.

This paper provides a detailed summary of the conference discussions and is presented in three sections: the first outlines the barriers to sharing information as identified by the conference participants; the second section explores the initiatives they subsequently proposed; and the conclusion outlines RUSI’s recommendations, as informed by the conference discussion, for taking this work forward to capitalise on progress made at the event.
A SCENARIO WAS PRESENTED to conference delegates that outlined a complex multinational money-laundering network and its discovery by a bank. The scenario prompted further discussions, illustrating some of the principal barriers to information sharing that preclude a more effective response to the challenge of illicit finance from law enforcement, regulators and financial institutions.

The Scenario

The international money-laundering network and bank, Mundus Bank, at the heart of the scenario are fictional. Any resemblance to real individuals, banks or businesses is coincidental. However, the money-laundering typology and barriers to effective information sharing and collaboration described are grounded in real-life experience.

Mundus Bank, with around 3,000 offices in both mature and emerging markets serves approximately 35 million customers in fifty countries and territories, and has correspondent banking relationships in a further 100 countries and territories. Mundus’s global footprint and scale mean that it processes 2 million cross-border transactions each day and files 100,000 suspicious transaction reports (STRs) annually.¹

There is inevitably suspicious financial activity hidden within these enormous volumes of legitimate trade. The scenario begins with Mundus’s detection of a pattern of round-figure payments – highly unusual in everyday transactions – into two of the bank’s accounts in Singapore, triggering a suspicious-activity alert within the bank. The subsequent Mundus investigation identified the following related trade and transaction flows:

- A Mundus account in Singapore received funds from a UK money service business (MSB). The originator was based in Latin America. The payments were for textiles, exported to Paraguay from China. In total, there were 102 payments between December 2013 and June 2014, amounting to $5.7 million

¹ A suspicious transaction report (STR, also known as a suspicious activity report) consists of information gathered by financial institutions (and other regulated sectors) on any identified suspicious activity and its author. These reports – generated if and when a suspicious transaction/activity is identified – are subsequently sent to the relevant national authority in charge of processing and investigating this information.
The same Mundus account in Singapore received funds from a non-Mundus account in Mexico, belonging to an individual. The payments were for electronics, exported to the US from China. In total, there were sixty-seven payments between September 2013 and June 2014, amounting to $3.3 million.

A Mundus account in Dubai sent funds to a second Mundus account in Singapore. The payments were for goods exported to Hong Kong from the United Arab Emirates (UAE). There were fifteen payments, amounting to €1.5 million and $0.5 million.

Analysis of this network revealed that it demonstrated little or no normal business activity and was marked by indicators of unusual financial activity in multiple jurisdictions. Only four Mundus account holders appeared to be part of the network. They operated in multiple and disparate lines of business. Their ‘know your customer’ profiles – information on individual clients – did not identify links to accounts in other jurisdictions.

A review of their transactions data identified non-Mundus accounts that played a significant role in the network. They were significant either because of the total funds they transacted to Mundus accounts and/or because of the frequency of their transactions. Research identified affiliated parties located in various jurisdictions (for example, directors). Some were in countries with poor transparency. For instance, the true source of funds paid out of the UK MSB was a Paraguay-based firm, with a nominee director domiciled in Panama.

Open sources claimed the nominee director was connected to other companies, but it was impossible to obtain the registration record to confirm the ultimate beneficial owner(s) or the nature of the business. Mundus’s investigation could not confirm whether the account holder was a front company for illicit financial activity. Similarly, some of the non-Mundus counterparties appeared to be holding companies registered in the British Virgin Islands. It was again impossible to determine the ultimate beneficial owners.

Continuing with the example of the UK MSB, more detailed investigation identified both concrete leads and barriers to information sharing. The MSB was known to Mundus Bank from a previous investigation into a Mundus account in Hong Kong, held by the director of the MSB. The director was investigated after law enforcement provided intelligence suggesting his account was involved in e-mail-hacking fraud. The UK investigative arm of Mundus discovered that the MSB’s director used to be a client of Mundus in another jurisdiction. Internal records showed that there was an internal investigation launched by Mundus Hong Kong. However, the UK team could not view the outcome of the investigation, which was the filing of an STR that ultimately led to the closure of the account. Hong Kong data-sharing rules do not allow for STRs to be shared outside the jurisdiction. This prevented the formulation of a holistic risk profile of the MSB and, to an extent, the network.

To summarise this investigation:

- Unusual transactions to a Mundus account triggered a system-generated suspicious-activity alert.
• Investigators identified that one of the main sources of funds into the first Mundus account was linked to a previous investigation
• They identified other Mundus accounts that received funds from the first Mundus account. Several Mundus accounts shared the same nominee directors, located in low-risk jurisdictions. Some accounts had been linked to previous money-laundering investigations in Mundus Turkey and the UAE
• The destination of funds from the ‘second’ Mundus account were non-Mundus accounts located in low-risk jurisdictions, apparently operating in incongruent industries. They also shared the same director as the first Mundus account
• Mundus was unable to determine the original source and ultimate destination of the funds.

This describes the ‘global’ view, but in practice no jurisdiction can achieve such a comprehensive overview of the network. For some the view is very limited indeed. This investigation identified four barriers to effective internal assessment and mitigation of risk, and to collaboration with external parties:

1. Each Mundus country office has to comply with local data-protection laws and regulations, which could prevent the bank establishing a complete picture of a client’s global footprint
2. A number of jurisdictions have transparency and secrecy restrictions, which prevent identification of the real people behind the accounts
3. Mundus Bank cannot discuss identified financial-crime risk relating to non-Mundus accounts with the banks where these accounts are held. This hinders Mundus Bank from finding and following critical illicit financial paths in a large network
4. Each jurisdiction files STRs to comply with local filing regulations. Each financial intelligence unit (FIU) sees only that part of the network that relates to its jurisdiction: there is no central body that sees all STRs and can communicate with or co-ordinate the law-enforcement response. Where transactions are with non-Mundus accounts in jurisdictions where Mundus has not filed (because there is no suspicious Mundus account in that jurisdiction) the local FIU and law enforcement will have no visibility of the network at all.

Analysis

The scenario was the catalyst for a discussion that identified the various challenges faced by private- and public-sector actors in the context of information sharing. Data-protection restrictions, insufficient resources, low levels of co-operation and inefficiency across the system were identified as the main challenges.

Data Protection and Sharing Restrictions

Since 1989, the Financial Action Task Force (FATF) has set the ‘International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF
These standards ensure the implementation of anti-money-laundering/counter-terrorist-finance (AML/CTF) measures throughout the globe and oblige governments to co-ordinate the reporting, investigation and prosecution of financial crime. The FATF provisions – Recommendations 20 and 21 – mean that the public and private sectors must divulge information collected in the normal conduct of business in order to aid and facilitate the combating of financial crime and terrorist finance. Obligations normally include reporting suspicious transactions, including personal and financial data referring to the subject of the suspected transaction, origin and destination of funds.

Recommendation 20, in particular, defines the obligation of the regulated sector to report any suspicious activity or transactions, while Recommendation 21 outlines the inability to disclose the reporting activity. However, while most FATF recommendations are accompanied by an interpretive note clarifying the meaning and intent of each requirement, this does not occur in relation to tipping-off (Recommendation 21). As a result, private-sector restrictions (or ability) to share the same information with partner institutions or branches in other jurisdictions were described as unclear and subject to different interpretations around the globe.

Although the overarching objective of international FATF regulations is to harmonise international efforts among governments, each individual state retains significant autonomy in determining how to enact those measures. Differences therefore exist regarding what should be shared, as well as which public and private institutions and jurisdictions can exchange information. As a result, harmonisation has not been well achieved and considerable jurisdictional variation persists. This is particularly true in relation to data-protection laws where each jurisdiction defines its own limited exceptions to permit data sharing in specific security, criminal or health-related situations. Participants argued that this hampers efforts to combat financial crime by creating different structures, rules and schemes through which information can be shared, thus preventing it from reaching all concerned parties.

For the private sector, these provisions restrict what can be shared with other regulated bodies, as well as with the public sector, in different jurisdictions. As it stands, while an international money-laundering network may be identified by a multinational bank, it is unable to share comprehensive details with any law-enforcement body, instead providing each jurisdiction with just the piece of the puzzle that falls within that state’s borders. Simultaneously, co-operation between national FIUs is conducted through requests for mutual legal assistance; but such requests can only be made once an FIU has identified which jurisdiction holds pertinent information. The process is far from rapid and information exchange remains subject to national data-protection restrictions.

3. Ibid., Recommendation 20.
4. Ibid., Recommendation 21.
International and national regulatory provisions – including those relating to data protection – therefore limit the circumstances in which a financial institution may share information with its counterparts, as well as how information may be shared across borders by both private and public bodies.

Adding to these restrictions, institutions must deal with issues regarding the ‘ownership’ of information, which determine accountability for data misuse. The updating, sharing and deletion of data can only be made by the entity which collects – and therefore, in effect, ‘owns’ – the information. As a result, difficulties can arise when considering information-sharing requests and needs. In this regard, participants agreed that only essential information should be shared, and that the ‘owners’ of information would remain responsible for ensuring that data is processed, protected and disposed of appropriately.

In relation to STRs, concerns regarding the potential violation of individual privacy are particularly acute. The threshold for suspicion is low, individuals are unaware that reports have been filed in their name and there is no supervised appeal procedure to rectify unfounded suspicion. Sharing such suspicions with multiple institutions therefore increases the possibility of individuals or companies being unjustly penalised and inadvertently creates situations of financial exclusion. From a commercial perspective, sharing this sensitive information is a logical step as it reduces the risk of facilitating illicit activity. Nevertheless, situations may arise where decisions are based on false suspicions that have been neither investigated nor prosecuted but, nonetheless, unjustly restrict access to the financial system. Doubts persist regarding the private sector’s ability and willingness to put fundamental rights ahead of business priorities. Moreover, the systems in place to allow individual consultation and revision of personal information are still underdeveloped in relation to existing requests for information sharing.

The ‘right to be forgotten’ may similarly be breached. This right states that ‘when you no longer want your data to be processed, and provided that there are no legitimate grounds for retaining it, the data will be deleted’. But how can this be ensured if data travels beyond the ‘owner’ to the various entities that request it or when the subject is unaware that the report exists? At present, the restrictions that ensure STR data cannot travel outside the public sector mitigate many of these concerns. If information sharing is to be broadened, the private sector must be

6. ‘Financial exclusion refers to a process whereby people encounter difficulties accessing and/or using financial services and products in the mainstream market that are appropriate to their needs and enable them to lead a normal social life in the society in which they belong.’ See European Commission, ‘Financial Services Provision and Prevention of Financial Exclusion’, 2008, chapter 2.

7. It is unlikely that the right to data erasure would apply in cases of suspected criminal activity. However, it is also unlikely that the retention of a suspect’s personal data for a long period of time without investigation, as currently happens with the majority of STRs, could be considered a necessary and proportionate application of the data-protection restrictions. This topic will be explored in more detail in a forthcoming RUSI CFCSS publication on data protection and financial crime.

ready to invest in mechanisms that ensure privacy rights are safeguarded to the same standard of transparency and accountability set by governments.

The conference plenary nevertheless concluded that the responsibility of private institutions to assist law enforcement needs to be accompanied by increased information-sharing powers in order to maximise the utility of collected data and capitalise on the resources dedicated by the regulated sector. With illicit actors often dispersing their activity between various institutions, the ability to share intelligence may enable illegal activity to be identified more rapidly. Participants noted that, within a more flexible information-sharing framework, the use of information for commercial purposes should be safeguarded, and issues regarding financial exclusion and the ‘right to be forgotten’ carefully considered.

Participants also suggested that interpreting the current legal framework is as great an obstacle as the provisions themselves. The uncertainty surrounding the legal requirements on what should and should not be reported leads to cautious, defensive reporting by the private sector. This consequently overburdens the public sector with unnecessary STRs.

Participants further emphasised that the private sector’s input into AML/CTF has grown exponentially, from unwilling actor to indispensable partner. It is time for regulations to catch up with these developments and facilitate private-sector action in this field. Overall, data-protection restrictions represent perhaps the most critical obstacle to information sharing, both between sectors and across jurisdictions; addressing this issue could therefore have a significant impact in improving the functioning of the system.

**Insufficient Resources and Excessive Costs**

Reporting requirements impose substantial costs on both the regulated sector and the law-enforcement bodies which must process the data received. The system is caught in a vicious cycle that stymies efficiency and effectiveness: the volume of data submitted means that the public sector lacks the resources to provide feedback or guidance, which creates limited confidence within regulated bodies, which therefore interpret requirements cautiously and submit an ever-increasing volume of reports.

Public-sector representatives from multiple jurisdictions identified inadequate staffing levels and out-dated IT systems as challenges that further exacerbate this problem. Lacking the staff numbers to review and develop all the intelligence received, public bodies are forced to prioritise areas of special interest or risk; financial intelligence (FININT), however valuable, is potentially lost in this process.  

Participants generally agreed that the level of public investment is greatly disproportionate to its impact on disrupting financial-crime networks; too much money is being spent with little evidence of it having a disruptive effect on criminal activity.

---

Limited resources have also contributed towards reduced interaction among the various public entities, contributing to poor co-ordination in investigations. Participants identified further inefficiencies when entering into dialogue with other public bodies outside those directly involved in the investigation. For example, an investigation sparked by an AML STR into illegal markets might find links to terrorist-financing activities, requiring collaboration with different teams. Lack of dialogue, however, often precludes this linkage, thus leading to duplicate investigations and an inefficient response to threats.

While law enforcement faces decreasing budgets, the private sector is investing significant amounts of resources into the identification of suspicious activity; however, without guidance or feedback, these resources could be misdirected.

It was agreed that information sharing between private and public actors is a lengthy, complicated and limited process which is inefficient and shows little evidence of success. The lack of dialogue and uncertainties surrounding reporting requirements were identified as important factors preventing the improvement of the system.

**Cross-Border Co-operation**

These challenges are amplified when investigations span national boundaries. First, the legal obstacles identified above present considerable challenges for a national FIU receiving an STR. STRs contain only information relating to the reporting jurisdiction, excluding any reference to the wider network. The national FIU must first identify which other jurisdictions may hold relevant information, and then try to gather enough data to file a sufficiently detailed mutual-legal-assistance or information request.

Second, the resource challenges identified create difficulties once a request has been submitted. Public bodies are forced to prioritise, and requests from international counterparts suffer, creating extended delays. Conference participants stated that despite FATF advice (in Recommendations 37 and 40) to have response mechanisms in place, authorities in most jurisdictions struggle to meet the appropriate timeframe to prepare and respond to requests. Consequently, authorities are rarely able to rely on internationally shared information to build an investigation; instead, its use is usually corroborative. Moreover, once information has been received from an international counterpart, its use is limited to the specific purpose stated in the request, rendering it useless to others who could potentially benefit from information therein.

It was widely acknowledged that international co-operation between public bodies is often unsuccessful and a frustrating exercise for all involved. Limited resources and poor co-ordination are exacerbated by the legal restrictions on the ways in which data must be processed. This reduces the ability of the different government agencies to collaborate with each other or survey data that could contribute to the effective handling of ongoing investigations.

---
Conference participants further highlighted that cross-border information sharing within the private sector is practically non-existent. Financial institutions bemoan the inability to provide their international counterparts with information that is visible to them and could, when combined with their own FININT, lead to the mapping of international criminal networks. Additionally, correspondent banking relationships (that is, where one financial institution is given the authority to act on behalf of another for the purpose of facilitating transfers) add a further level of complexity: while correspondent banks do have an obligation to request information on clients, specific requirements vary from jurisdiction to jurisdiction and therefore do not necessarily provide all the information necessary to the identification of suspicious activity.

Unable to share client information across borders, large multinational banks, and other regulated entities, therefore cannot comprehensively rid their operations of the threat of criminal interference (‘de-risk’). Within the current FATF-inspired provisions – widely adopted across mainland Europe and the UK – a financial institution that is aware of illicit activities in an international correspondent branch is not permitted to disclose that information with those branches and therefore must either allow the illicit activity to continue, or break data-protection and tipping-off laws. This has consequences for the institution, and facilitates continued illicit activity and the survival of transnational organised criminal networks.

In sum, information-sharing provisions were not conceived as part of an international system incorporating both public and private dimensions; as a result, they have significantly increased the costs of compliance. The length of time that public bodies take to respond to the requests of their counterparts, the inability of a financial institution to prevent illicit funds tainting its own business and the disjointed everyday relations between domestic actors, are each a consequence of the poor planning given to regulating exchanges of data across borders. Increased co-operation would, ultimately, facilitate a new and efficient international model for information sharing. Its inclusion in the framework would not only contribute towards increased dialogue but also better co-ordination and implementation of policies across the board.

Effectiveness: The Principal Casualty

The legal restrictions, lack of resources and poor co-operation emphasised during the conference unavoidably lead to ineffectiveness in the international fight against financial crime.

First, the lack of harmonisation across jurisdictions and with regard to both data-protection legislation and AML/CTF requirements, creates a challenge to all those trying to share information. The confusion surrounding what may and should be shared, and what constitutes suspicious activity, invariably leads to defensive action by the private sector and, ultimately, to unnecessary reporting and poor FININT.

Second, without sufficient resources to guide and analyse FININT, investigations do not profit from the process as much as was intended by regulators. The reporting system is not just a tool for tackling financial crime; it should also contribute to combating a wider range of criminality. However, the information available is rarely used to this effect. The resource insufficiency that
plagues the public sector also reduces the impact of the considerable private-sector investment, which is not targeted or exploited effectively.

Third, whether due to data restrictions, inefficient use of resources or a lack of co-ordination, international co-operation is beset by obstacles in both the public and private sectors, further undermining both effectiveness and efficiency.

The global AML/CTF regulations promoted and maintained by FATF have placed the private sector at the centre of the battle against financial crime, responsible for implementing measures that monitor, analyse and report on all suspicious activity that takes place in the context of its operations. This ‘privatisation of control’ means that law enforcement depends on the private sector to carry out initial investigations and obtain crucial evidence. However, the inefficiency of the current system is closely linked to the regulatory contradiction that holds private-sector actors responsible for identifying criminality and providing evidence, but does not empower them to act within the full spectrum of their abilities. Without the ability to share information, domestic and international counterparts tasked with combating financial crime are forced to work with incomplete FININT. Participants therefore suggested that addressing this contradiction at the various identified levels would offer a number of advantages to both the law-enforcement departments receiving STRs as well as to the private sector’s own efforts to safeguard against financial crime. It would permit a more sophisticated assessment of criminal trends and tools: better use of FININT; a reduction in demands on public resources; and facilitation of international co-operation.

Overall, participants concluded that enhanced information sharing between private, law enforcement and government bodies depends on improved co-ordination, more efficient allocation of resources, better use of collected information and a refocusing of regulatory regimes to target effectiveness rather than just compliance.

II. Towards a New Model for Information Sharing

PERSPECTIVES GATHERED DURING the conference suggest that, fundamentally, information-sharing provisions need to be updated for the twenty-first century. Whether in terms of tools, strategies, actors or dynamics, the current system was created in a context with few international transactions, lengthy communication processes and where little interaction was expected between different jurisdictions or actors.

The importance and relevance of sharing information among all involved in the fight against financial crime is unquestionable. However, the tools in place have, unfortunately, failed to evolve with the criminality they seek to prevent.

In addition to identifying the failures of the current system, participants also proposed possible initiatives, providing detailed and insightful clues to what the future in this field should look like and in what ways the various stakeholders may contribute to its construction. Participants supported the pursuit of an approach that favours effectiveness and shared responsibility.

Clearer and More Comprehensive Laws

It was suggested that FATF standards, their implementation by governments and domestic data-protection provisions are less prohibitive than commonly perceived. While restrictions and obstacles exist, participants said that a simple clarification process providing additional guidance would be sufficient. Interpretation of legal requirements should be addressed at the international level in order to facilitate the harmonisation of legal frameworks and diminish obstacles caused by current differences.

Participants were particularly keen to find solutions tackling the inability of private institutions to share STRs with each other under statutory protection from prosecution. At the national level, a solution inspired by Section 314(b) of the US Patriot Act received the most support.1 Safe-harbour provisions under this section allow for ‘voluntary information sharing’ among some financial institutions in order to promote the identification of money-laundering or terrorist activities. This exchange is ultimately directed at improving the value of reports and ensuring the regulator receives more accurate and partly processed information. It offers advantages for the public and private sectors, and has been used to process a total of 2,576 requests for information sharing to date.2

---

Within jurisdictions, the US model is a positive example that warrants further examination. Of particular note is the speed with which information must be processed and shared under this section, the inherent legal protection provided to the participant regulated sector and the ability to discover which other bodies participate in the programme.

In its implementation, the US regulator – the Financial Crimes Enforcement Network – applies strict provisions to the use of information. Sharing between private entities is restricted to ‘Identifying and, where appropriate, reporting on activities that may involve terrorist financing or money laundering; determining whether to establish or maintain an account, or to engage in a transaction; or assisting in compliance with anti-money laundering requirements.’ Similarly, the safe-harbour principle applies only to participating entities. Broadly, Section 314(b) facilitates a stronger working relationship between the public and private sector and has increased the quality of information deriving from the private sector’s improved reporting and enhanced communication as agreed and described by conference participants.

The principles underpinning Section 314(b) are certainly promising from the perspective of facilitating information sharing. Conference delegates highlighted how this model could serve as a potential example for other jurisdictions, contributing towards better co-operation, resource utilisation and efficiency.

However, this is still a very US-specific measure that falls under the legal exceptions created after the 9/11 attacks; as such, it may face some difficulty in being transferred to other jurisdictions. Taking the UK as an example, the public sector faces considerable difficulties processing information within current timeframes, as well as maintaining up-to-date records and responding to requests made by the regulated sector; this provision’s application to the UK would therefore appear set to fail unless accompanied by an appropriate increase of resources.

Furthermore, when considering the international implications, the measure’s voluntary nature means that it does not favour harmonisation of information-sharing practices, as advised by international regulations. Although some success might derive from it, its application to the international system would need to be reviewed and adapted to suit international law and general standardisation requirements.

Broadly speaking, existing laws and regulations lack the assumption of ‘trust’ between sectors as well as a straightforward and internationally harmonised implementation framework. The advantage of Section 314(b) is that it is a vote of confidence in the private sector and provides the appropriate protection to those that contribute to tracking down and identifying criminals. As such, with some adjustments provided, it would be a welcome addition to other information-sharing provisions in other states.

---

Increased Resources

At the conference, the public sector was often mentioned as a less-than-willing partner and, even at a domestic level, appears to hold a poor record for facilitating exchanges of information. Whether the result of limited resources or internal procedures, the conference plenary agreed more needs to be done to improve the public sector’s ability in dealing with the information it holds.

At a domestic level, more staff and better use of FININT were highlighted as the most effective solutions. It was also suggested that the information exchanges of public-sector departments could be easily improved by a greater understanding of the utility that specific information may have to the different parties. Software that enables different parts of the public sector to access collated FININT, albeit filtered subject to clearance levels, might offer an interesting tool. Through such a system, public officials would not depend on the time and resources of their counterparts, as the bulk of information needed would be readily available and accessible through a simple and secure login system.

Innovative software solutions are often cited as the key to achieving a better use of FININT and improved information sharing. The European Commission’s FIU.Net programme—a ‘decentralised computer network supporting the FIUs in the EU in their fight against Money Laundering and Terrorist Financing’4—shows promise and addresses many of the data-protection obstacles that have been highlighted.

The programme, which is soon to be transferred to EUROPOL premises, uses Ma3tch, innovative software that enables governments to search the STR databases of their partners.5 Crucially, it does this without the need for a shared database and without transmitting any personal information outside the jurisdiction, instead ‘convert[ing] FIU data into uniform anonymised filters’ for searching.6 It is therefore a tool that enables law enforcement to establish which other governments hold relevant information in order to submit a request for mutual legal assistance.

The underlying objective behind this type of software is to contribute to the more effective use of FININT, more efficient use of resources, increased co-operation between jurisdictions and greater compliance with international data-protection provisions.

The use of software similar to Ma3tch would significantly assist stakeholders as it overcomes data-protection regulations through the removal of data fields that might reveal unnecessary personal information. In the EU’s upcoming data-protection revision the concept of “Privacy by

---

design’ and ‘privacy by default’ will ... become essential principles in EU data protection rules’.\(^7\)

Its basic principle – the ability to share information omitting all personal and identifiable data – is in fact already being transposed to national jurisdictions, as shown in the UK by the work of the Information Commissioner’s Office.\(^8\) As a result, the differentiation between transaction data and personal data will most likely by heightened, leading to increasing reliance on programmes that allow for information sharing without interfering with individual rights.

Within the resources debate it was also suggested that the issue of data overload, misinterpretation of what must be reported and the quality of information provided in reports could be improved through an increase in guidance specifying domestic and international priorities, criminal trends and typologies of interest. If the regulated sector understands where and how it needs to focus its actions, reporting will naturally become streamlined.

To this end, a greater emphasis on risk-assessment exercises at national and international levels would be essential. These reports would generate frequent updates on the main threats to financial stability and security. Typologies derived from these assessments should be adapted to provide biannual guidance to the regulated sector regarding which specific transactions and financial activities to monitor and report on with increased detail. A two-tier system whereby reported activities would fall under ‘priority’ and ‘all suspicious transactions’ was suggested as a potential solution to help manage data, focus resources, increase the regulated sector’s clarity on what is required by law and, ultimately, improve the quality of reporting.

The resourcing challenges would benefit from the partnership-oriented approach widely advocated by participants as key to a new information-sharing model. A more collaborative response to the lack of funding, limited staffing and out-of-date IT tools could be an effective solution and cement government trust and relationships with private-sector actors.

**Greater Emphasis on Co-operation**

At the national level, the obstacles to information sharing are mostly linked to the absence of dialogue between actors. A partnership approach to increase co-operation between public- and private-sector actors received strong support. Facilitating domestic trust-building systems was therefore welcomed by participants and could lead to important structures for co-ordination between financial institutions under the guidance of law enforcement.

The UK’s Joint Money Laundering Intelligence Taskforce (JMLIT) is a good example of efforts to this end. Within this task force, the National Crime Agency facilitates co-ordination with and between private-sector institutions, providing an environment in which they are allowed to collaborate and operate in a constructive manner. The response to the JMLIT initiative has been a


success, highlighting that while market positioning is a natural concern for financial institutions, and is often cited as a barrier to sharing information with competitors, it should have little impact on their actions in responding to financial crime. As supported at the conference, JMLIT allows its participants to share relevant information without the risk of having it used against them. It is a safe-harbour situation akin to the US 314(b) provisions.

However, when considering the JMLIT as an example, it must be acknowledged that it is a limited pilot programme operating in relation to individual cases and including only certain banks. Widespread co-operation is necessary and would need to include a broader membership within the private sector in the UK and elsewhere.

At the international level, the Toronto-based Egmont Group is an informal gathering of FIUs. With regard to international information-sharing systems, it is the most developed platform and helps member governments exchange data and co-operate in cross-border investigations. In practice, Egmont’s mandate is to function as a bridge between countries through its ‘Egmont Secure Web’, which allows for safe information sharing and is the only international FIU co-operation platform. However, Egmont is not a universal institution and, due to its relatively Spartan structure, does not currently have the ability to expand and support governments in training and operational needs.

The conference plenary agreed that reinforcing the Egmont Group would be an important step towards improving the frequency, efficiency and quality of inter-state information sharing. As governments are increasingly restricted by reduced resources and staff, international co-operation is among the first type of activity to suffer. The empowerment of the Egmont Group with the appropriate resources to manage and adequately safeguard the information shared internationally would greatly facilitate international co-operation in tackling financial crime. Moreover, doubts regarding the safety of information would also be reduced as Egmont would be endowed with updated software and information-sharing systems; however it should be noted that some parties held reservations on how appropriate this solution was.

The Egmont Group was also suggested as a model for private-sector co-operation at the international level. A similar institution for the private sector would allow regulated entities to share information through a secure system and ensure its members comply with international standards. The Wolfsberg Group, an elite group of the world’s largest banks, could perhaps lead by example and play an expanded and more inclusive role in this regard. By developing more evidence-based solutions and guiding principles for international collaboration, Wolfsberg members could demonstrate best practice through their shared interests and willingness to co-operate. With time, the system could expand to other financial institutions and the remaining AML regulated sector.

International co-operation is a crucial element of a revised information-sharing model, which is ultimately dependent on the willingness of governments to collaborate and invest in systems that facilitate the process while respecting national differences. International bodies such as FATF or the Egmont Group should therefore be given additional powers to co-ordinate these efforts and generate specific practical measures that can be adopted swiftly and effectively in collaboration with the private sector.

**Effectiveness**

The cumulative effect of the obstacles identified above is an inefficient system. Conference participants emphasised that a new model should be focused on effective action, and on the wider aim of disrupting and ultimately stopping criminal activity. Participants agreed that, in reality, it is systemically difficult to achieve convictions as a result of financial investigations and under current financial-crime legislation. In the majority of jurisdictions the predicate offences – the actions from which illicit money derives – are the criminalising element which ensure convictions and, in fact, reduce crime. FININT-based information-sharing systems are, therefore, best used as tools for law-enforcement action as effectiveness derives from their success.

It was agreed that the solutions proposed above, such as clearer laws, effective resourcing of public bodies and increased co-operation, may not lead to a substantial increase in convictions. However, the improvement of the information-sharing model should facilitate the tackling of illicit flows going through the financial system and an effective disruption of predicate offences. This would be welcome progress to all regulated entities, as well as law enforcement and governments.
III. Conclusion: A Blueprint for Information Sharing

CONFERENCE PARTICIPANTS AGREED that a new model for information sharing is required to overcome the challenges identified and outlined previously. Drawing on these discussions, this paper recommends a new model, which is guided by the principle of **effectiveness** and based on three pillars: a clear legal framework; improved resourcing; and facilitated co-operation between public and private sectors and internationally. Specific recommendations under these pillars are outlined below.

**Effectiveness**

An overarching theme across these pillars is the use of FININT. Governments must learn to set priorities and communicate them to the private sector in order to ensure better quality reporting and contribute to the joint improvement of the legal framework. This would create a virtuous circle of increased effectiveness, as more appropriate strategies for disruption and prevention are developed, and more productive dialogue fostered with different stakeholders.

With the support of the research community, governments and law enforcement should therefore actively work with the private sector to:

1. Generate evidence-based research to further develop the concept and operational use of FININT.

**Pillar One: A Clear Legal Framework**

Revised data-protection provisions, or more effective guidance on the interpretation of current laws, will play a crucial role in improving the information-sharing system.

Data-protection laws must, at all stages, be accompanied by a sense of accountability. Governments and the private sector alike must offer reassurance by being publicly responsible – for example with regard to individual privacy – for the gathering, processing and updating of collected data for the purposes of combating financial crime. As we evolve into an increasingly international system, jurisdictional limitations will gradually diminish. Without the state to protect individual rights, any future system must therefore be reliant on international standards that ensure equal safeguards and obligations regardless of nationality or jurisdiction. A comprehensive, standardised and clear set of data-protection provisions is therefore much needed.
To this end, governments should consider two measures:

2. Promote and disseminate information and guidance that clarifies data-protection requirements in the context of fighting financial crime
3. Request that the FATF revisit its recommendations on reporting, FIUs and tipping-off in order to provide mechanisms for information sharing within the private sector. The FATF also needs to take a more active role in emphasising the importance of information sharing, perhaps including an assessment of this activity in its mutual evaluations.

Pillar Two: Improved Resourcing

The resources and staff available to the public sector to tackle financial crime were deemed insufficient and inadequate by the majority of attendees. In particular, there is a significant lack of resources for managing the substantial increase of STRs that are now submitted each year not only in the UK, but across most jurisdictions. The result is inefficient and unco-ordinated action – both within and across governments – as well as limited feedback to the regulated sector.

The conference proceedings emphasised the need to provide the public sector with adequate resources, while simultaneously allowing the private sector to expand its information-sharing capabilities. Increased feedback and dialogue from the public sector, alongside the ability to co-operate and share information with other private institutions, would enable the regulated sector to provide better quality, more comprehensive and targeted information. Increased resources within the public sector would therefore have a force-multiplier effect on the overall effort, enabling public bodies to capitalise on the significant investigative power and capability of the regulated sector.

Innovative technology-based resources will also be crucial in facilitating a new information-sharing model. The identified obstacles include the inability to process high volumes of data, of different types and from multiple sources; finding an instrument that is able to process all this information within a secure and effective system is essential. Conference conclusions suggest that further analysis is needed into the use of ‘privacy-by-design’ tools like FIU.Net’s Ma3tch that could be developed and expanded beyond the EU. The adoption of systems able to facilitate efficient information sharing while simultaneously protecting individual rights would be an important first step towards developing a new model.

To support this pillar, governments should commit to four key measures:

4. Provide regulators and law enforcement with sufficient tools, resources and updated technology to operate effectively and fulfil their guidance role
5. Create regional bodies to facilitate information sharing across jurisdictions, using the FIU.Net model. These bodies should also be empowered to promote co-operation across groups and intra-group jurisdictions, forming a strong international network
6. Develop Ma3tch or similar privacy-by-design software for global adoption by each of these regional FIU.Net bodies to support both their individual roles and their co-operation
7. Partner with the private sector to enhance the availability of resources (for example through funding) to support information sharing.

**Pillar Three: Facilitated Co-operation**

Finally, improving and increasing co-operation between all participating actors and, particularly, jurisdictions will be paramount. Governments and the private sector should invest in a partnership approach that builds on permanent dialogue and exchange of information. Future efforts should focus on providing frameworks for dialogue and encouraging organisations such as the Egmont and Wolfsberg Groups – co-operative bodies consisting of FIUs and major banks respectively – to assume a greater leadership role for the public and private sectors respectively.

To achieve this, governments and the private sector should work together to:

8. Hold Wolfsberg Group-like bodies responsible for providing guidance to their members and establishing co-operation mechanisms that permit safe and effective data sharing. In essence, such organisations would reach beyond current membership and build towards a private-sector ‘Egmont’ function

9. Establish further initiatives based on the UK’s JMLIT model, increasing the platforms for dialogue between the public and private sectors

10. Support policy-making at FATF and national levels that is based on prevention and specific disruption objectives to avoid overburdening the system with defensive reporting and lengthy investigative practices.

Finally, governments should:

11. Increase the Egmont Group’s role as a pillar of international co-operation, in the context of information sharing, and revise national strategies for communication between public bodies.

Implementing these recommendations would increase effectiveness in the global fight against financial crime and represent significant strides towards a new model of information sharing based on public–private co-operation.
Annex: Prepared Notes of Keynote Speech

The keynote speech was delivered by Jennifer Shasky Calvery, Director, Financial Crimes Enforcement Network, US, 27 May 2015. A transcript of the prepared remarks appears below.

Good morning. I would like to thank the Royal United Services Institute for the opportunity to attend this important workshop, and speak with you this morning.

I think we can all agree that the public sector faces a daunting challenge in simply identifying – let alone confronting – the illicit finance networks impacting our national and international security. The reporting provided by our financial institutions plays a central role in enabling us to understand the flow of illicit funds through the international financial system. However, if we expect to keep pace with networks adept at employing increasingly complex and ever shifting means to move illicit funds, it is right that we should be here together exploring the benefits we might gain by maturing our public-private approach and enhancing multilateral information sharing.

I will seek to build upon the discussion yesterday in which colleagues so poignantly, not to mention prolifically, identified the challenges we face. I will now seek to pivot the discussion toward solutions.

Setting the Context

To bring things back into focus this morning, let me begin with a quick review of the threats we are facing. They are quite serious and provide the context for why we must work together effectively.

Today, there is perhaps no greater threat than the one posed by al-Qa’ida, the Islamic State in Iraq and the Levant (ISIL), their respective affiliates, and in particular by those individuals seeking to go to the region to fight for terrorist groups. Yet, our threats are also multiple, extending far beyond terror finance. They include rogue nations, foreign grand corruption, and increasingly serious cyber threats, as well as transnational criminal organizations, including those involved in the global narcotics and human trafficking trades, and massive fraud schemes targeting our governments, businesses, and people.

One thing each of these threat actors have in common is the need to move funds while hiding their nature, source, location, and ownership. Thus, they are susceptible to strategies that disrupt their sources of revenue, restrict their access to the international financial system, and
impose sanctions on their financial facilitators, particularly if it is employed as one aspect of a wider, comprehensive whole-of-government approach to the problem.

Let me begin with a tangible example in the terrorist-financing arena. The U.S. Government is executing a comprehensive, whole-of-government strategy to disrupt, degrade, and ultimately defeat al-Qa’ida, ISIL, and other terrorist groups. We are actively engaged in the broad Global Coalition to Counter ISIL, a group of over 60 countries and inter-governmental organizations dedicated to working together. The Treasury Department takes the lead on the financial component of U.S. efforts, collaborating closely with our counterparts in the State Department, the Department of Defense, federal law enforcement, and the intelligence community.

But to be clear, the financial component is only one strand of wider efforts involving a range of elements, including traditional law enforcement strategies around arrests, prosecutions, and forfeiture actions.

The emergence of ISIL, its affiliates, and the flow of foreign terrorist fighters to the Iraq and Syria region has required the development and implementation of new and creative approaches to counter terrorist groups’ fundraising and financial operations, both at a strategic and tactical level. At the strategic level, the Treasury Department’s efforts to degrade ISIL’s financial strength are focused along three mutually supportive elements. First, we are working to disrupt ISIL’s revenue streams to deny it funds. Second, we are working to limit what ISIL can do with the funds it collects by restricting access to the international financial system. And third, we continue to impose sanctions on ISIL’s leadership and financial facilitators to disrupt their ability to operate. Within this strategic framework, FinCEN plays an important role.

Thanks to the reports filed by financial institutions, FinCEN has a wealth of data that we are able to analyze and disseminate in the form of financial intelligence to our Treasury colleagues, and to law enforcement and intelligence community partners. The information provided by financial institutions allows us to connect the dots between seemingly unrelated individuals and entities. These capabilities are critical in supporting the U.S. Government’s efforts to disrupt ISIL sources of revenue, to restrict their access to the international financial system, and to impose sanctions on ISIL facilitators.

Financial institution reporting also provides us with critical information that has helped us identify foreign terrorist fighters, their supporters, and their financial networks overseas. Disrupting the flow of foreign terrorist fighters and their facilitators is also a U.S. counterterrorism priority and a key line of effort in our counter-ISIL strategy. There is no doubt at FinCEN, or amongst our partners across government, that the reporting financial institutions provide results in a rich collection of high value information. It is essential to our efforts to disrupt, degrade, and ultimately defeat al-Qa’ida, ISIL, and other terrorist groups.

In fact, the reporting financial institutions provide is essential to our efforts to disrupt, degrade, and ultimately defeat the full spectrum of illicit organizations presenting criminal and security threats. It is at the heart of what is now commonly referred to in government policy circles as
threat finance and financial intelligence. And, just as importantly, it is built on the backbone of our existing anti-money laundering and countering the financing of terrorism (AML/CFT) framework, including our ongoing public-private partnerships.

The Role of Financial Intelligence Units (FIUs) and Financial Intelligence

Nearly every country around the world has anti-money laundering (AML) and countering the financing of terrorism (CFT) laws in place at this point. These laws are meant to protect the integrity of the financial system by leveraging the assistance of financial institutions to make it more transparent and resilient to crime and security threats, and to provide information useful to law enforcement and others to combat such threats.

Under the international standards set by the Financial Action Task Force (FATF), FIUs serve as the national center for the collection of suspicious transaction reports (STRs) and other information relevant to money laundering, associated predicate offenses, and terrorist financing. The precise sources of financial reporting collected by FIUs vary from jurisdiction to jurisdiction. In addition to the required collection of STRs, common sources of reporting collected by FIUs include: threshold transaction reports; international funds transfer instructions; certain information on law enforcement investigations; and various ad hoc and targeted collections.

The reporting collected by an FIU is generally a rich collection of high value information. Its value derives from the following qualities:

- **It is Comprehensive**: The FIU dataset reflects inputs from diverse stages of the money flow cycle and from a wide array of financial ecosystem participants. As a result, it offers the potential to identify and track illicit funds flows across national barriers, and regardless of financial sector, institution, intermediary, or transmission method used.
- **It is Significant in Size and Scope**: The significant size and scope of the FIU dataset permits the creation and use of predictive models to identify emerging global funds flow trends and anomalies.
- **It Contains Specific Identifiers**: The FIU dataset is remarkable in its richness of identifiers. Critically, these are not simply names but often unique identifier numbers that make the financial intelligence strongly actionable.
- **It Includes High Quality Human Intelligence**: One source – the STRs – leverages the efforts of thousands of financial sector participants (i.e., individual human sources) uniquely positioned to identify potential illicit activity. The best STRs tell compelling narratives that have already been vetted and researched to the extent possible under applicable laws and regulations.
- **It can be Supplemented with Targeted Collections**: FIUs generally have the ability to supplement their routinely collected datasets with targeted, supplemental collections. The circumstances under which FIUs can pursue supplemental records, the precise methods used to collect them, and the sources from which they can be collected vary by jurisdiction depending on the applicable laws and regulations.
Under the FATF standards, FIUs also serve as the national center for the analysis of their financial institution reporting. Each FIU is staffed with individuals that have at least a minimum level of expertise in their sources of reporting and the analysis thereof. Several FIUs have advanced levels of expertise but it varies from jurisdiction to jurisdiction.

FIUs are staffed with analysts that specialize in working with the reporting collected from their particular sources, including most prominently domestic bank and nonbank financial institutions. FIUs are often staffed with highly knowledgeable specialists who spend years sifting through the high volume of reporting filed by their financial institutions. Their deep familiarity with their sources and proximity to the underlying collection efforts provide FIU analysts with unique insights and opportunities to further their own analysis and that of their partners. Additionally, some FIUs are also responsible for regulatory, supervisory, or law enforcement functions that provide their analysts with additional sources of information and areas of expertise.

The best FIUs combine external sources of reporting – including open source, law enforcement sensitive, and intelligence information – with their internal sources of reporting to produce finished financial intelligence reports for law enforcement, regulatory, policymaker, and private sector audiences. When done well, their reports identify emerging threats to the global financial system by piecing together the money laundering methods, networks, nodes, and rails used by illicit actors.

However, FIUs are only as good as the quality, depth, and volume of the reporting we receive from our financial institutions and other reporting entities. Our effectiveness as FIUs, and thus the very foundation of our threat finance strategies, depend upon it. It is important that we continue to push ourselves to ensure that we are collecting meaningful reporting and supplementing it with our analysis to produce actionable intelligence.

The Potential of the Egmont Group

I would like to turn to the Egmont Group of Financial Intelligence Units and introduce it as a potential aide for maturing our public-private approach and enhancing multilateral information sharing. The Egmont Group’s infrastructure provides its member FIUs, and by extension their many public and private partners, with access to a global platform for seeking and disseminating financial intelligence across approximately 150 jurisdictions. The attributes of this government-to-government, global platform are unparalleled, and include:

- A Transparent, Legal Basis for Collecting and Sharing Intelligence: To become an Egmont Member, an FIU must be established by the jurisdiction’s laws and meet the FATF standards. As a result, each FIU has a transparent, legal basis for collecting financial intelligence and exchanging it with other FIUs abroad, thereby minimizing the heightened privacy concerns inherent in non-transparent or covert activities.
- A Common and Secure Technology Connection between Member Jurisdictions: Egmont Member FIUs use a common technology system, the Egmont Secure Web (ESW), to send encrypted communications containing financial intelligence bilaterally or share financial
intelligence multilaterally through encrypted, online ‘communities of interest.’ All of the
approximately 150 FIUs that participate in the Egmont Group have access to the ESW,
which is administered by FinCEN.

• **A Network Intended to Benefit Third Parties:** The Egmont Group’s governance
documents explicitly encourage the widest range of international cooperation, assume
dissemination of financial intelligence to third parties, and provide a framework to
ensure the protection and confidentiality of information shared between FIUs. The only
other limiting factors are those imposed by the originating FIU and a jurisdiction’s laws.
Since each FIU already has an extensive network of public and private partners within
its jurisdiction, the Egmont Group connects these approximately 150 networks with one
another, for the potential benefit of all.

• **Clear Operating Rules and Disciplinary Process:** The Egmont Group’s governance
documents provide further protections by setting forth the rules on the use and
dissemination of exchanged financial intelligence, the minimum physical security
requirements and degree of operational independence for an FIU, and the disciplinary
process for violating the Egmont Group’s rules.

So we have built a global platform that could provide the backbone for engaging in the type of
information sharing contemplated by the conference scenario, i.e., public-private, multilateral
information sharing. The potential is there. It needs to be tapped.

FIUs and law enforcement have been capitalizing on the Egmont platform. I do not want to
give the impression it is not used. It is used rather extensively and successfully. Indeed, it has
been used and tested over the space of two decades. It is just that until some recent efforts
I will discuss more in a moment, we have limited ourselves to more modest goals. We have
been using the Egmont platform almost exclusively for bilateral information sharing to support
reactive law enforcement investigations when the potential is really much broader.

However, the Egmont platform also should not be viewed as a panacea. While the Egmont
Group’s governance documents encourage the widest range of international cooperation,
individual FIUs are still limited by the restrictions contained in their national laws, particularly
those related to privacy and confidentiality, and even some that are not authorized to engage
in multilateral information sharing, just bilateral. Thus, it is important that we continue to
work through standard setting bodies such as the Financial Action Task Force and domestic
authorities to strike the appropriate balance between security-related information sharing on
the one hand, and privacy and confidentiality on the other.

**Experimentation as the Basis for Advancement**

Thus far, I have been talking about existing strategies, existing authorities, existing capabilities,
and existing infrastructure. I thought we were meant to be talking about new models, paradigm
shifts, and revolution. What is going on?
Well, let me begin by saying that I have never been known as a defender of the status quo. Quite the contrary, I have built my work history around start-ups, rebuilds, and implementing mandates for change. If you walk into my office, you will see a quote from Winston Churchill in large block letters covering the better part of a wall stating, ‘To improve is to change; to be perfect is to change often.’

Instead, I am a proponent of continuous hypothesis-driven experimentation, iterative pilot projects, and validated learning within the existing operating environment. I believe such an approach shortens the timeline for change, even what ultimately proves to be comprehensive change, and lowers the risk of failure. We do not have the luxury of creating things from scratch. We all operate in an existing paradigm and have demands upon us right now. Indeed, we are talking about rebuilding the engine to this car while driving it full speed down the highway.

Start talking about new models and paradigm shifts and you may very well see things grind to a halt. We have well-worn clichés to describe the phenomenon: ‘paralysis by analysis’ or ‘allowing the perfect to become the enemy of the good.’ It is the point where opposition becomes entrenched in the status quo. Instead, talk about pilot projects, experimental learning, proof of concept exercises, and incremental building on proven successes, watch everyone visibly relax. Don’t be surprised if even the most notorious curmudgeon grudgingly begins to discuss the art of the possible.

I would suggest to you that we have already entered an era where such experimentation has become the order of the day. I see it happening by and between FIUs, law enforcement, financial institutions, and regulators. I can readily think of examples involving the FIUs of the United States, Canada, Australia, UK, Netherlands, South Africa, Mexico, and Colombia. These are positive developments that should be encouraged and their results should be studied and successes adopted, adapted, and combined in ever-evolving combinations to address specific threats.

This morning I will discuss a few areas of ongoing experimentation. They are the ones with which I am most familiar by virtue of my position as the Director of FinCEN but they certainly are not the only examples of innovation and progress. Indeed, I applaud RUSI for attempting to catalogue these ideas through this workshop and encourage you to spread your outreach further for there is certainly innovation occurring in the AML/CFT space in a range of jurisdictions and by a range of public and private organizations.

Yesterday, we heard from our UK colleagues about their Joint Money Laundering Intelligence Task Force, a one-year pilot program they are pursuing to encourage real-time, iterative information sharing between the government and financial institutions on serious criminal and security threats. In the United States, we have been pursuing pilot initiatives and are considering yet others with objectives similar to the UK effort, using the statutory authority granted to FinCEN in Section 314 of the USA PATRIOT Act.

Under Section 314(a), the government and industry are granted authority to share with one another information related to money laundering and terrorist financing. Under Section 314(b),
financial institutions are granted authority to share such information amongst themselves under a safe harbor that offers protections from liability. Financial institutions subject to an AML program requirement under FinCEN regulations, and any association of such financial institutions, are eligible to share information under Section 314(b). That includes banks sharing information with other banks, casinos, money services businesses, insurance companies and securities and futures brokers.

Historically, we have used Section 314 for fairly modest purposes given the strong foundation it provides for public-private and private-private information sharing related to money laundering and terrorist-financing. Thus, as interest has grown in both the public and private sector to find ways to improve our information sharing about specific and significant threats to the financial system, and to do so on a more real-time and iterative basis, a renewed interest in Section 314 has likewise grown.

FinCEN has responded by sponsoring various pilot initiatives to explore the utility of Section 314 for these purposes. The goal of each individual effort is to learn new methods for information sharing, methods that are more effective and efficient than our current way of doing business, through hands-on experimentation on actual financial crimes threats. In this way, we hope to discover methodologies that can be syndicated and applied more systematically, pursuant to Section 314, by public and private institutions in the United States.

We also seek to share the insights we are gaining on particular financial crimes threats through these and other initiatives via FinCEN’s Financial Institutions Advisory Program so that other financial institutions can use the information to improve their AML/CFT efforts. To that end, FinCEN has worked with some larger financial institutions to develop ‘red flags’ about types of threats and then disseminated that information more broadly through public and non-public advisories. Two relatively recent examples of this focused on red flags associated with the illicit use of funnel accounts and the movement of funds associated with human trafficking or smuggling.

Another tool we are using as a generator for hypothesis-driven experimentation is the Bank Secrecy Act Advisory Group (BSAAG). The Bank Secrecy Act (BSA) is the name of the statutes and regulations that comprise the U.S. AML/CFT laws in the United States. The BSAAG, consisting of representatives from regulatory and law enforcement agencies, financial institutions, and trade groups, is the means by which Treasury receives advice on the operations of the BSA. It has approximately thirty private sector members from individual financial institutions and trade associations, each of which serve a three-year term and represent a broad cross-section of the size, location, and type of financial institutions covered by the BSA.

As chair of the BSAAG, the Director of FinCEN is responsible for ensuring that relevant issues are placed before the BSAAG for review, analysis, and discussion. The group is exempted from the normally applicable sunshine laws to encourage candid discussions among participants about the challenges we face in implementing our AML/CFT regime. Indeed, it was through the BSAAG that the idea for greater use of Section 314 originated and developed into the current series of pilot initiatives. The group also continues to explore ideas on how government can best:
communicate financial crimes priorities to industry; align the work of the public and private participants in our AML/CFT regime; minimize any gap between efforts expended on threats versus vulnerabilities; and create beneficial feedback loops between government and industry.

FinCEN has also been leading the charge on the greater use of coordinated multilateral collaboration to address global criminal and national security threats, working with both regional and global partners. Most recently, these initiatives have focused on the threat of foreign terrorist fighters associated with the so-called Islamic State in the Levant. The Egmont Group of FIUs is supporting this expedited multilateral collaborative effort of 24 Egmont member FIUs. Since the project’s inception in February 2015, participating FIUs have shared financial intelligence, strategic reports, and other ISIL-related information while identifying important characteristics of the financial transactions and activity of FTFs as they travel to and from the conflict zone. As a formal test case for multilateral information sharing and the role of FIUs in national terrorist financing efforts, the project also has identified two significant areas requiring further national and multilateral legal and policy action: lack of sufficient access by many FIUs to relevant national information and legal limitations preventing financial institutions from providing their multinational view of terrorist financing networks to all affected jurisdictions.

Conclusion

In closing, let’s recognize that financial intelligence has taken on greater relevance than ever before in supporting comprehensive multilateral strategies focused on serious international security issues. Let’s also recognize that our financial institutions go to great expense to provide reporting crucial to those strategies. So discussions such as this one, which are focused on how to improve and be more effective in our work together, are important. Thank you for the time and contributions you have made to our collective thinking on information sharing through this workshop.
Clare Ellis is a Research Analyst in the National Security and Resilience Group at RUSI. Her research interests include counter-terrorism, organised crime and security-sector reform in post-conflict states. She is also interested in the changing demands on UK policing, including its role within the national-security framework and as part of international-development missions. Prior to joining the Institute she worked in the criminal-justice sector, first within criminal defence and later within the police. Clare holds an MSc with distinction from the Department of Security and Crime Science at University College London, where her dissertation examined the spatial and temporal distribution of terrorism incidents in post-accord Northern Ireland. She has also studied at the University of Newcastle and the Université Lumière Lyon II, holding a Bachelor’s degree in Law with French.

Dr Inês Sofia de Oliveira is a Research Fellow with the Centre for Financial Crime and Security Studies at RUSI. Her research interests include the international regulation of money-laundering activities and financial crime, the financing of terrorism and proliferation finance, as well as illicit trafficking. Prior to joining RUSI, Inês lectured on International Relations and International Law at the University of St Andrews and the University of Edinburgh. Previously, Inês worked in Brussels in public affairs dealing with European law, public policy and governance.

Inês holds a PhD in Politics from the University of Edinburgh where her research focused on the international anti-money laundering regulations and the role of international organisations in the policy-making process. Inês further holds an LLM in International Law from the University of Edinburgh where her dissertation focused on the EU efforts to combat international drug trafficking. She also holds a degree in International Relations from the University of Coimbra and studied European Affairs at the University of The Hague.