SUMMARY OF EVENT DISCUSSION –

Brussels Roundtable

The Future of Financial Information-Sharing Partnerships in Europe

DATE OF EVENT: Tuesday, 9 Jan 2018

About:

The Future of Financial Intelligence Sharing (FFIS) research programme leads independent research into the role of public-private financial information-sharing partnerships (FISPs) to detect, prevent and disrupt crime. The FFIS programme is a research partnership between the RUSI Centre for Financial Crime & Security Studies and NJM Advisory.

This summary of discussion of the *'Brussels Roundtable on the Future of Financial Information-Sharing Partnerships in Europe'* has been prepared by the FFIS research team. This roundtable event was held on a Chatham House-rule basis.[1] As such, views and recommendations expressed in this paper reflect the authors' summary of discussion and should not be taken to reflect the views of RUSI, specific individuals or institutions that participated in the event.

Contact: For further information about the FFIS research programme, please visit www.future-fis.com or contact the organisers by email.

[1] When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

Summary of discussion:

This roundtable event included representation from: The Association for Financial Markets in Europe (AFME); Anti-Money laundering Europe (AME) professionals; Central Bank of the Netherlands; Citi Bank; Deutsche Bank; European Commission; EUROPOL; EY; FIU-the Netherlands; HSBC; IIF; National Police of the Netherlands; Privacy International; RUSI Centre for Financial Crime and Security Studies; Standard Chartered Bank; Thomson Reuters; Transparency International EU; UK HM Treasury; Western Union.

Initial speaker remarks were made by:

- **Che Sidanius,** Global Head of Financial Regulatory & Industry Affairs, Thomson Reuters
- **Nick Maxwell,** Head of the Future of Financial Intelligence Sharing (FFIS) programme, RUSI
- **Hennie Verbeek - Kusters,** Head FIU-the Netherlands
- **Rob Wainwright,** Executive Director, EUROPOL
- **Erik Barnett,** Regional Head of Europe, Financial Crime Threat Mitigation, Financial Crime Risk, HSBC;

Roundtable discussion covered:

- National-level developments in the Netherlands to support information-sharing between the public and private sectors to tackle serious organised crime and terrorism across Europe;
- Innovations and ongoing challenges for the role of transnational financial information-sharing organised through EUROPOL; and
- Coherence issues between data protection and financial crime policy priorities in Europe.

Overall, there continues to be innovation at the national level and transnational level across Europe in tackling serious crime and terrorism through information-sharing. The impact of public/private financial information-sharing partnerships in improving arrest and seizure rates in the UK, Hong Kong, the US and Australia has been noted in Europe. The FFIS study 'The Role of Financial Information-Sharing Partnerships to Disrupt Crime' recommendations were recognised as valuable for the European policy context; recording early experience in the UK, USA, Hong Kong, Singapore, Canadian and Australian of public/private information sharing.

There was broad acknowledgement of the importance of learning from the range of national examples. Funding has been made available at the EC level to support this period of innovation. DG HOME have an active Call for Counter-Terrorism Proposals to Member States, including support for public-private partnerships. (see below for details)

The Netherlands experience of developing a financial information-sharing partnership (FISP) may provide a model to other European countries to establish pilot partnerships within existing data-protection legislation exemptions. This may be a reference example for countries without specific enabling legislation for public/private financial information-sharing, such as exists in the UK or the USA. Comments reflected the importance of, at least, using the existing legislative provisions in each national context to improve the quality of feedback to the regulated sectors on suspicious reports. The Netherlands example provided insight into the value for law enforcement in providing more detailed feedback to the regulated sector.

The Netherlands-FIU experience noted that, beyond immediate operational value to law enforcement of single reports of suspicion, the analysis of the database of transactions held by the FIU can inform intelligence on macro-trends, typologies and modus operandi of major criminal and terrorist threats. As such the intelligence yield of the individual reports can be greater than their immediate operational use by law enforcement agencies in active investigations.

Discussion in detail

Systemic challenges…

The EUROPOL findings were presented from the "FROM SUSPICION TO ACTION" - Converting financial intelligence into greater operational impact" (EUROPOL, 2017) study. The report highlighted that, at the EU level, the AML/CFT regime generates millions of suspicious transaction reports annually, however, only around 10% of these reports lead to further investigation by competent authorities. Europol estimates that barely 1% of criminal proceeds in the European Union are ultimately confiscated by relevant authorities.

Several comments reflected on deficiencies in the current reporting framework in the AML/CFT system. Overall, the quality and relevance of the majority of suspicious reporting of money laundering and underlying crimes in Europe are not felt to be fit for purpose. Suspicious Activity Reports (SARs) or Suspicious Transactions Reports (STRs) fail to provide actionable operational intelligence on a suspect of interest, to draw out all the relevant information on a suspect from within a financial institution, or help provide a macro-understanding of the financial crime risks.

Banks can provide a more comprehensive intelligence picture on suspects than are required within a SAR/STR (including recent photos from cash machines, IP addresses, financial information, geographic movement through use of cards). With appropriate time and resources, private sector analysts can observe linkages via transactions; identify networks; develop risk-based scenarios; and validate the findings through in-depth investigations.

A number of comments reflected on the dis-proportionate nature of the current reporting framework. Representatives from the regulated sectors believed that current regulatory incentives in Europe encourage over-reporting on customer transactions because the current regulatory incentives (in practice) on financial institutions are to report customers rather than take a targeted approach. Some stakeholders described how this dynamic can encourage de-risking/de-banking of groups based on generic indicators of suspicion and highlighted examples how parties that were later found to be innocent had been victim to de-banking. Discussion covered how the AML/CFT system could move towards targeted reporting, targeted client account closures and targeted 'keep open' procedures for accounts, depending on what is of most value to law enforcement investigations.

Stakeholders discussed the challenges for the growing use of artificial intelligence (AI) within financial information sharing partnerships, particularly in ensuring that any AI systems for identifying risk and suspicion did not reflect inefficiencies and bias in human judgements made within historical data.

Innovation in the Netherlands...

In the Netherlands Financial Intelligence Unit (FIU-NL) experience, different levels of public/private information-sharing have been achieved, according to different levels of confidentiality, as follows:

1. **Low confidentiality level:** The FIU-NL works with a range of industry partners to produce guidance information on threats. Information sharing at this low-level of confidentiality is focused on information sharing with obliged/regulated entities through bulletins and guidance.
2. **Mid confidentiality level:** FIU-NL and the Dutch Banking Association (NVB) have formed a Terrorist Financing (TF) Platform. This level of information-exchange revolves around discussion and sharing insights on threats, feedback on Suspicious Unusual Transaction Reports (SUTRs) and consultation on the drafting of risk profiles. These can then be shared with other reporting entities as guidance at the 'low confidentiality' level. At the same confidentiality level, the FIU-NL supports cooperation with the Dutch association of Money Transfer Companies (NVGTK) and is developing a code of conduct with specific ML & TF indicators and due diligence measures for the money service bureau sector.
3. **Highly confidential:** FIU-NL engagement on specific subjects of interest with specific financial institutions, at an operational level including 'pre-attack' investigations. This information exchange takes place under authority of Article 18 of the Dutch Policing Code, with oversight from the Ministry of Security and Justice. As such the information-exchange at this confidentiality level must be specific, goal oriented, documented, in accordance with a work instruction for the handling of data, time-bound and subject to evaluation.

At the most advanced confidentiality level, the level of diligence taken around data handling is very high and must meet a substantial public interest test. This approach has typically been directed at counter terrorism operations, but could also apply to a range of serious crimes.

The Netherlands pilot will be formally evaluated within the next 6 months. However early challenges include having an appropriate IT solution as there is a wide variety of IT used by partners and therefore a lot of manual transposition work required. It was noted that the political drive towards this information sharing has been centred on counter terrorism. Political support will be required to use the same tools to tackle serious organised crime groups. There is an aspiration to develop the Netherlands model to broaden the engagement to different private sector actors. FIU-NL is also involved in test driving a multilateral reporting pilot and multilateral analysis of financial intelligence.

In roundtable discussion, it was noted that most EU Member States will have an exemption in data protection regimes, similar to Article 18 of the Dutch Policing Code, to achieve a similar approach as is currently being trialled in the Netherlands.

Transnational understanding of financial crime threats in Europe...

EUROPOL has prioritised building analytical power by combining multiple sources and providing analysis at a transnational level in Europe. Through this approach, a new level of macro understanding about crime threats has been achieved. However, despite the huge cost and strength of architecture for suppressing criminal finances, it is noted that the current scale of disruption of crime through the financial system provides no real deterrent to serious and organised criminals as a whole (though counter terrorist financing is working more effectively).

Data protection regulations can have unintended consequence of limiting FISPs. European legal regimes are believed to present a number of barriers to such information-sharing at the transnational and cross border level in particular. It is noted, by comparison that criminals operate internationally at ease and are highly adept at forming international networks to facilitate money laundering.

To help respond to these challenges, EUROPOL has launched a High Level Forum (HLF) to support information-sharing at the transnational level with some of the Europe's largest banks. The HLF operates a senior level with banking leaders, is convened with support of the Institute of International Finance (IIF) and has hosted a number of operational level meetings. The focus of the HLF has been to identify blockages in the legal and regulatory system to achieve specific CTF/AML information-sharing objectives and, secondly, to share typologies and strategic understandings of the threat.

Funding for innovation...

There continues to be innovation in practice at the national level and transnational level across Europe in tackling serious crime and terrorism through information-sharing, and further initiatives and funding are available at the EC level to support this period of innovation. The European Commission is investigating and supporting research that seeks to understand blockages to supporting more cross border information flow to tackle the terrorist financing risks.

DG HOME have an active Call for Counter-Terrorism Proposals to Member States, including support for public-private partnerships, under the ISF-Police fund opened on 29th November. The period for applications is open until 6th March 2018. The objective is to support the development of public-private partnerships between private entities, FIUs and law enforcement to facilitate the exchange of information about terrorism / terrorist financing, in a collaborative and secure environment, as well as a network of CT financial investigators to reinforce the effectiveness of financial investigations in terrorism cases.

Participants can find more information in the in the following link, where there is also a link to the text of the call: http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/isfp/topics/isfp-2017-ag-terfin.html . Any questions about the call shall be sent to the following email address: HOME-ISF@ec.europa.eu.

10 recommendations raised by participants throughout discussion:

1. Regulators should send clear signals that public/private information-sharing to improve understanding of financial crime risks is supported and encouraged within the regulatory system. The behaviour of regulated entities is driven by the regulator, not necessarily by law enforcement interests. It can be legal and beneficial to law enforcement, but if the partnership approach is not reinforced by regulatory signals, then financial institutions will struggle to adopt it.
2. The AML/CFT reporting regime in general should move towards more targeted reporting, guided by real suspects of interest to law enforcement, rather than over-reporting based on 'fear of missing something' or 'better safe than sorry'. Guidance to help prioritise reporting on specific AML threats may also help achieve more proportionate reporting.
3. The overall reporting regime could be improved by moving towards providing intelligence on suspect customers, rather than a single line of 'activity' or transaction. This would include sharing of wider amounts of customer information and network analyses, not just raw data, on (likely a smaller number of) targeted suspects.
4. Much more work is required across EU Member States to achieve alignment between law enforcement priorities, and FIU, regulator, supervisor and data protection authority signals to the private sector. The implementation of the EU General Data Protection Regulation (GDPR) presents a moment to define good practice in this regard. EC and Members States should work together to define 'what good looks like' in achieving policy and regulatory coherence between data protection and financial crime objectives, including developing harmonised definitions for information-sharing, and may require specific enabling clauses in implementation legislation.
5. Over time, across Europe, FIUs and major SAR/STR reporters should be moving toward co-location of public and private financial crime investigators. This is believed to have worked well in the other fields, such as cyber security and in protection against child exploitation. Vetted bank employees, when co-located can provide real-time intelligence to law enforcement to prevent and respond to terrorist attacks and serious criminal activity. Legislation or guidance should be considered in Europe that allows for pooling of relevant bank data and analytical capabilities to enhance intelligence picture; i.e. private/private sharing alongside public/private sharing.
6. Agencies in Europe should be examining US 'Keep Open Account' procedures, where accounts are identified as suspicious but kept open in order to support an active law enforcement investigation. In the UK, a voluntary code for 'keep open' is being developed.
7. Further policy and research thinking is required to understand whether the rise of technology in financial crime analytics (within a broader policy discussion about predictive policing) is increasing or formalising any bias within historic data or historic investigations. The lack of data on what it means to be 'effective', given the low overall performance figures in AML, mean that it is difficult to 'train' artificial intelligence systems without reinforcing historic bias.
8. Law enforcement and the FISPs across Europe should focus more on professional enablers of money laundering and financial crime. The emergence of 'Crime as a Service' professional groups has been noted by EUROPOL and they demonstrate increasing sophistication in their understanding money laundering regulations in order to evade them. Transparency International is leading a taskforce for professional groups which seeks to support policy thinking and private sector integrity and practice in this regard.
9. In terms of the future development of FISPs in Europe, there may be a case for developing individual partnerships to deal with particularly difficult issues or geographies (Gaza, Syria etc).
10. As future issues to consider, the growth and emergence of telecommunication companies as financial service providers should be carefully considered in the context of their responsibilities to identify financial crime.

This event is part of the Future of Financial Intelligence Sharing (FFIS) programme, delivered by the RUSI Centre for Financial Crime & Security Studies and NJM Advisory;

A number of governments around the world have committed to developing public-private financial information-sharing partnerships that bring together law enforcement agencies, regulators and the financial sector to detect, prevent and disrupt financial crime. The Future of Financial Intelligence Sharing programme is an independent series of events and research that seeks to build the evidence base for understanding 'effectiveness' in the context of information-sharing, share good practice and identify emerging lessons from around the world in this rapidly developing area of anti-money laundering practice and policy.

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges. Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 185 years. *London | Brussels | Nairobi | Doha | Tokyo | Washington, DC*

The International Advisory Committee for the Future of Financial Intelligence Sharing programme:

- Laure Brillaud, Transparency International EU
- Rene Bruelhart, President of the Financial Intelligence Authority of the Holy See
- Jennifer Shasky Calvery, Global Head, Financial Crime Threat Mitigation, HSBC
- Chris Costa, Global Chief Operating Officer, Fraud Investigation & Dispute Services, EY LLP
- Matt Ekberg, Senior Policy Advisor for Regulatory Affairs, Institute of International Finance (IIF)
- Max Heywood, Tackling Grand Corruption Programme, Transparency International Global Secretariat
- Paul Horlick, Director - Head of Financial Intelligence Unit (FIU) at Barclays Bank
- Geraldine Lawlor, Global Head of Financial Crime, Barclays
- Nick Lewis OBE, Group Head, Integrated Intelligence and Investigations, Financial Crime Compliance, Standard Chartered Bank
- Rick McDonell, Executive Director of ACAMS
- Tracy Paradise, Executive Secretary, the Wolfsberg Group
- Dr Bill Peace, University College London
- Che Sidanius, Global Head of Financial Regulatory & Industry Affairs, Thomson Reuters
- Ben Trim, Head of Financial Crime Policy, Group Public Affairs, HSBC
- Malcolm Wright, Chief Compliance Officer, Revolut: The Global Money App

---

Supported by:

HSBC

the answer company™ THOMSON REUTERS®

EY Building a better working world

WESTERN UNION WU