ICLG

The International Comparative Legal Guide to:

Business Crime 2019

9th Edition

A practical cross-border insight into business crime

Published by Global Legal Group, in association with CDR, with contributions from:

AGS Legal
Allen & Gledhill LLP
Anagnostopoulos Criminal Law & Litigation
Atsumi & Sakai
Bogatyr & Partners
Clayton Utz
De Pedraza Abogados, S.L.P.
De Roos & Pen
Debevoise & Plimpton LLP
DSM Avocats à la Cour
Enache Pirtea & Associates S.p.a.r.l.
Global Financial Experts Limited
Homburger
Hrle Attorneys
Ivanyan & Partners
Kachwaha and Partners
Lawfirm Holzhacker
Lutgen + Associés
Maples and Calder
Matheson
Navigant Consulting, Inc.
Paksoy
Peters & Peters Solicitors LLP
Rahman Ravelli
Rogério Alves & Associados, Sociedade de Advogados, RL
Skadden, Arps, Slate, Meagher & Flom LLP
Sołtysiński Kawecki & Szlęzak
Studio Legale Pisano
Tanner De Witt
TripleOKLaw LLP
Uroš Keber – Odvetnik
Vilardi Advogados Associados

CDR Commercial Dispute Resolution

glg global legal group

global legal group

Contributing Editors
Keith Krakaur & Ryan Junck, Skadden, Arps, Slate, Meagher & Flom LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Sub Editor
Hollie Parker

Senior Editors
Suzie Levy
Caroline Collingwood

CEO
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd
September 2018

ISBN 978-1-912509-33-1
ISSN 2043-9199

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

The Developing Partnership Between Financial Institutions and Law Enforcement

Claiborne (Clay) W. Porter

Navigant Consulting, Inc.

Robert Dedman

Introduction

Financial institutions of all types, regulators, and law enforcement across the globe recognise the vital importance of information sharing in the fight against terrorism and financial crime. Experience has shown that efficient, timely information sharing by a bank, broker-dealer, or a money services business (MSB) with law enforcement can often help prevent a terrorist attack or dismantle a crime syndicate.[1] Indeed, according to the Financial Action Task Force on Money Laundering (FATF), which was founded in 1989 on the initiative of the G7 to develop policies to combat money laundering (ML), "[E]ffective information sharing is one of the cornerstones of a well-functioning anti-money laundering/counter-terrorist financing (AML/CTF) framework".

A. *Required Information Sharing vs. Public-Private Partnerships*

Information sharing through formal reporting requirements and statutorily required committees composed of law enforcement and members of the financial services industry is the typical mechanism through which these entities share information. As a general matter, this method of information sharing is most often in the form of information being passed from the financial institution to law enforcement – the financial institution reports suspicious activity to law enforcement, or another regulatory authority.

Public-private partnerships, on the other hand, are a two-way street. Typically set up in the form of a committee or a working group, these partnerships have representation from both the public sector (federal, state, and/or local law enforcement and regulatory authorities) and the private sector (banks, MSBs, broker-dealers, and other financial institutions). Membership in the partnership may often depend on the committee or working group's area of focus, such as financial crime typologies. Ideally, it is intended that information flows freely in these partnerships among the members, and each member reaps a benefit from participation. For example, if typologies are the focus, banking representatives share information with law enforcement on a specific ML typology they have found in their compliance work. Law enforcement and regulators would in turn share information that would help the bank when identifying certain typologies or schemes related to typologies, which may help the banks adjust and adapt their transaction monitoring or refine how their financial intelligence unit (FIU) is conducting investigations into these typologies, as appropriate.

B. Current Trends in Public-Private Partnerships

In the United States, statutorily mandated information sharing, such as Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs), has existed since the advent of the Bank Secrecy Act (BSA) of 1970. Public-private partnerships between financial institutions and law enforcement, where members of banks and law enforcement convene to discuss current trends in anti-money laundering enforcement, have existed about the same amount of time, though most are informal and often on an *ad hoc* basis.

With the passage of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), public-private partnerships have taken on greater importance as financial institutions and law enforcement working to enhance their cooperation in the fight against terrorist financing and financial crime. And in the past five years, as BSA and sanctions enforcement increased, many financial institutions have been requesting a greater emphasis to be placed by the U.S. government on public-private partnerships.

Outside of the U.S., the concept of public-private partnerships has already taken root, as foreign banking regulators crack down on money laundering and terrorist financing (ML/TF) in their jurisdictions and regulators become more active.

The intent of this chapter is to identify the current information sharing mechanisms and the public-private partnerships existing today and offer potential reforms designed to further improve the process. To be sure, informal and confidential public-private partnerships addressing immediate threats are always taking place – this chapter, however, is devoted to public partnerships that address systemic ML/TF compliance efforts.

History of Information Sharing Between Financial Institutions and Law Enforcement

Information sharing can be divided into two broad categories: statutorily mandated information sharing; and information sharing in the form of public-private partnerships, where law enforcement and industry come together to discuss matters such as certain ML typologies, risks, and best practices for prevention. These partnerships are formal and informal – from organised meetings with select bank members to informal exchanges of information between a broad range of financial institutions and law enforcement.[2] As public-private partnerships have grown in value and sophistication, they now often appear to be at the forefront of proposed reforms in the U.S. and the focus of some foreign law enforcement initiatives to tackle financial crime.

A. Mechanisms for Sharing Information between Financial Institutions and Law Enforcement

In the U.S. and the United Kingdom, statutorily mandated information sharing between law enforcement and financial institutions is a linchpin of AML/CTF law.

1. United States: The Role of the BSA and the USA PATRIOT Act Section 314(a)

In the U.S., the BSA and the USA PATRIOT Act both explicitly mandate information sharing with law enforcement.[3] The filing of SARs, first required in the BSA and then further expanded in the USA PATRIOT Act, are for the direct benefit of law enforcement and other public-sector enforcement authorities.[4] For example, Section 314(a) of the USA PATRIOT Act specifically states that a federal, state, local, or foreign law enforcement agency investigating ML/TF may request that the U.S. Department of the Treasury, Financial Crimes Enforcement Network (FinCEN)[5] solicit, on its behalf, certain information from a financial institution or a group of financial institutions.[6] Since 2015, FinCEN has sought to enhance the standard 314(a) requests with case-specific contextual briefing for institutions assessed by FinCEN to possess relevant data. Typically, 314(a) contextual briefings take place approximately every six weeks with up to 10 cases reviewed each year.[7]

Another example of U.S. statutorily mandated information sharing is the Bank Secrecy Act Advisory Group (BSAAG). In March 1994, BSAAG was established by the U.S. Treasury Department pursuant to the Annunzio-Wylie Anti-Money Laundering Act of 1992. The BSAAG serves as a forum for the financial industry, regulators, and law enforcement to communicate about how SARs, CTRs, and other BSA reports are used by law enforcement and how the record keeping and reporting requirements can be improved in an effort to enhance their utility while minimising costs to financial institutions. BSAAG organisation members are selected by the secretary of the treasury to serve a three-year term with an individual designee of the organisation representing that member at biannual plenary meetings.[8]

2. United Kingdom: Section 7 of the Crime and Courts Act 2013

Like the U.S. and other jurisdictions, there is always formal and informal sharing of information between UK law enforcement and UK financial services firms. Of particular note, the Crime and Courts Act 2013 established the National Crime Agency (NCA), which replaced the Serious Organised Crime Agency, and includes a section that explicitly allows disclosure of information to the NCA if the disclosure is made for the purposes of the exercise of any NCA function. Section 7, which allows the NCA to share information with third parties, is also the legal basis for the NCA's participation in one of the leading information sharing public-private partnerships in the UK, the Joint Money Laundering Intelligence Taskforce (JMLIT).[9]

In February 2015, the JMLIT was established as an NCA initiative created in public-private partnership with the financial sector to tackle high-end ML. It was developed with partners in government, the British Bankers' Association, law enforcement, and over 20 major UK and international banks. A management board oversees JMLIT's activities and reports to the Financial Sector Forum,[10] the NCA, and the Financial Conduct Authority (FCA), with ultimate oversight by the UK Home Office, a ministerial department supported by more than 30 agencies and public bodies.[11] The JMLIT's primary objectives are to:

a. Improve the collective understanding of the ML threat (Detect).

b. Inform the prosecution and disruption of ML activity (Disrupt).

The JMLIT's two main working groups, the Operational Group and the Expert Working Group, seek to identify vulnerabilities in the UK AML/CTF system. Specifically, in 2016 and 2017, the JMLIT and its groups were credited with multiple operational outcomes, including 63 arrests of individuals suspected of money laundering and the forfeiture of 7 million pounds of suspected criminal funds.[12]

3. Suspicious Transaction Reporting Globally

Like the U.S. and the UK., many countries' AML/CTF laws include a requirement to share information with law enforcement and/or regulatory authorities. In fact, the legislative requirement to report suspicious activity to law enforcement entities is almost universal. Nearly all FATF-member countries have enacted legislation to require:

a. The criminalisation of money laundering.

b. Reporting of suspicious transactions.

c. The establishment of an FIU.

d. International law enforcement cooperation and information exchange agreements with non-U.S. governments.

It should be noted that the establishment of such legislation, however, does not necessarily imply full compliance with international standards.[13]

For a chart of countries requiring the filing of suspicious transaction reports and the AML/CTF legislation for each country, *see* **Appendix A**.

B. FATF's Consolidated Standards on Information Sharing and Existing Public-Private Partnerships

Internationally, many countries are stepping up information sharing between public-private entities in response to nearly 30 FATF recommendations and the requirements of seven Immediate Outcomes in the FATF Methodology for assessing effectiveness.[14] In particular, FATF's recommendations focus on facilitating access to, and sharing of, beneficial ownership information and relevant information on nonprofit organisations.

1. Specific FATF Recommendations on Information Sharing

FATF recommends that financial institutions and their directors, officers, and employee should be:

a. Protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory, or administrative provision, if they report their suspicions in good faith to the applicable FIU.

b. Prohibited by law from disclosing or tipping off the fact that a suspicious transaction report or related information is being filed with the FIU.[15]

2. Notable Public-Private Partnerships and Best Practices

Six countries currently have public-private partnerships consistent with FATF recommendations worth noting here: Australia; Canada; Hong Kong; Singapore; the UK; and the U.S. Of these six, Australia and the UK provide interesting examples of the public-private information sharing partnership model. The other partnerships, such as the U.S.'s BSAAG, will be discussed below. For a detailed breakdown and comparison of the six countries' public-private partnerships, and their potential limitations, *see* **Appendix B**.

a. Australia's Fintel Alliance

To date, the Fintel Alliance appears to be the only example where law enforcement and industry participants are co-located in "hubs" and have access to analytical IT resources. Such a setup likely has been key to the Fintel Alliance's success as it provides for "actionable real-time intelligence".[16] Publicly launched in March 2017, the Fintel Alliance is led

by the Australian Transaction Reports and Analysis Centre (AUSTRAC), which serves as the Australian FIU, as a public-private partnership between government agencies and private financial institutions. The Fintel Alliance partnership includes AUSTRAC, as the supervisor, six banks, a major digital money transmitter, a money-service bureau, and multiple law enforcement agencies. The Fintel Alliance also invites international law enforcement authorities to engage as members of the Operations Hub (see below), such as the UK's NCA.

Additionally, the Fintel Alliance consists of "Operations Hubs" and "Innovation Hubs", which allow law enforcement and financial industry professionals to collaborate on cases and engage in focused dialogue, as well as to work on "creative business models and design new AML/CTF controls in their changing environments."[17] Such collaboration also is designed to build trust and confidence among the participants.

b. UK's JMLIT

A key element of any successful partnership is a consensus on goals and objectives among the participants and stakeholders. Tackling financial crime seems to be no different. A coherent strategic approach among the participating public-private institutions appears to be of critical importance. The UK's JMLIT is an example of such a functional strategic alignment, as the JMLIT's thematic priorities follow from the UK National Risk Assessment[18] process. Specifically, the JMLIT's priorities reflect strategic law enforcement priorities and consultation with regulated entities on threat priorities.

Existing Practices

Public-private partnerships may take on many forms and shapes, and there does not appear to be a one-size-fits-all type of structure that can work for all nations and institutions with varying profiles and footprints. Financial institutions may establish relationships directly with their local law enforcement agencies. Regulators and governing bodies may seek support from their international peers who are farther along in building their AML/CTF regimes.

Certain elements, however, frequently emerge as best practices in the public-private information sharing model. In addition to real-time access, co-location, and the strategic alignment of goals and priorities, common themes among successful partnerships include the following:

A. Tone-at-the-Top

Tone-at-the-top has shown to be a cornerstone of a successful national financial information sharing partnership, just like it is a foundation of an effective and functional AML/CTF compliance programme. High-level support from political and business stakeholders is one of the key principles of a successful financial information sharing partnership programme. A mandate for the public-private partnerships seems to help enable the participants to work under a shared objective and dedicate significant resources and efforts.[19]

For example, the UK Home Secretary sets the tone-at-the-top by mandating relevant enforcement agencies to engage with JMLIT. Additionally, JMLIT's crossover of personnel between the public-private sector has seemed to help facilitate trust and confidence, as well as alignment of national law enforcement, private sector, and JMLIT priorities.[20]

B. Robust Governance Structures and Oversight

Examples of well-designed public-private working arrangements include:

1. JMLIT's Management Board: fulfils governance functions and reports to the Financial Sector Forum, which consists of senior leaders from regulators, government, banks, and other stakeholders.
2. Fintel Alliance: publishes a detailed Member Protocol, covering objectives, governance, information security, vetting, and dispute resolution arrangements.
3. The FinCEN Exchange: a voluntary public-private information sharing partnership for law enforcement and financial institutions that aims for law enforcement and FinCEN to share typologies learned on illicit finance threats with financial institutions to help them identify illicit activity and for the financial institutions to provide law enforcement with feedback on SARs.[21,22,23]

C. Technology and Analytical Capability

The use of technology is also a key part of a financial information sharing partnership design. Experience has shown that AML/CTF partnerships are more likely to be successful when they use and aspire to develop new technological solutions for real-time threat sharing and responses to information requests. For example, one of the key missions of the Fintel Alliance is to enable innovative systems of financial transactions and payments to emerge through its Innovation Hub. The Fintel Alliance also benefits from a dedicated Foundations Program Board, which helps shape its strategic direction, including IT innovation and tools.[24]

Suggested Enhancements in the U.S.

In the U.S., true public-private partnerships appear to be in the very beginning stages of formation, with the contours yet to be decided. The FinCEN Exchange is a helpful start and will hopefully be a harbinger of more public-private partnerships. As these initiatives crystallise into full partnerships, the following recommendations will maximise their usefulness.

A. Real-Time Dialogue and Feedback Loops

Real-time dialogue and a consistent feedback loop between law enforcement and private sector financial institutions.

Feedback Loops

A true public-private partnership will be a continuous feedback loop – a two-way street – where feedback from law enforcement and regulators to financial institutions on whether the SARs they are filing, and the typologies they are using, are relevant and useful to investigations, and financial institutions are adjusting approaches and sharing additional information based on the law enforcement feedback. The need for a better feedback loop between law enforcement and regulatory authorities and the private sector is not a new recommendation for reform, but it grows increasingly necessary in today's environment. For example, the Clearing House[25] recently suggested that better coordination and communication between law enforcement and financial institutions would help "reconcile competing U.S. government priorities and align their effect on financial institutions, while creating efficiencies".[26]

In addition to feedback to financial institutions on what is useful (and not useful) in their SAR filings, regularly scheduled meetings among financial institutions and law enforcement where law enforcement highlights highly valuable SARs (on an anonymous basis), or where there is concern that highlighting a particular SAR may reveal an investigation, highlight the typology of a certain scheme found in the SAR and further discuss the portion of the transaction that the bank cannot see (anonymously). These meetings could provide the private sector invaluable information on how to conduct their reviews and investigations of potentially suspicious activity.

B. The FIU "Sandbox" and Safe Harbor

Forming effective public-private partnerships may require some legislative fixes and cooperation among the various regulators and law enforcement agencies.

1. Legislative Recommendations and Remedies

Industry professionals and organisations, including the Clearing House, have suggested that FinCEN propose amendments to the Safe Harbor provision in the USA PATRIOT Act. Recommended amendments include a broader definition of activity to include other types of crime and a broader scope of parties covered by Safe Harbor, including technology companies and other nonfinancial services firms.[27] These amendments are designed to assist the private sector by clearly stating the boundaries around what information may be shared and with whom, and what information cannot be shared.[28]

Another method proposed by industry professionals and organisations to increase information sharing through legislation is the creation of an FIU "sandbox" – a shared utility or database of SARs and SAR information that could be accessible not just by law enforcement and regulatory authorities, but by certain cleared individuals from private financial institutions. The purpose of the FIU sandbox would be the free exchange of information on potential suspicious individuals and entities for the sole purpose of detecting and preventing financial crime.

2. Other Options

Other options could include the use of formal agreements or service level agreements among law enforcement, regulators, and financial institutions to allow financial institutions to provide data and information on trends and patterns of observed customer behaviour without liability for potential programme or reporting failures. Another option is the creation of working groups and/or committees dedicated to specific trending topics, such as the use of machine learning in detecting financial crime, which would meet on a regular basis (e.g., monthly) and include representatives from the financial industry, law enforcement, and regulators. A larger working group or committee could also be created to focus on law enforcement and regulatory priorities and trends emerging from ongoing investigations and reviews, like the FinCEN Exchange, to better convey information on these subjects back to private industry. Working through these data privacy concerns will likely always be a challenge with sharing information between law enforcement and the financial services industry and will therefore need to be closely reviewed as sharing agreements are formalised.

Conclusion

Criminals engaged in money laundering and other financial criminal activity are continuously inventing new ways to try to evade law enforcement and escape detection by financial institutions. For decades such criminals have leveraged inefficiencies and fragmented information sharing to bolster their illegal activity. To improve the chances of defeating such illegal activity, law enforcement, regulatory, and private-sector responses must come in a similar dynamic and innovative fashion. The current domestic and international information sharing partnership approach appears to be a turning point in the right direction, but continued reform to innovate the frequency and flow of information is necessary and must be imminent. Further, experience has shown that information sharing partnerships can improve their effectiveness by focusing their efforts on building more trust and promoting the free flow of information between public-private institutions, with the intention of taking a collective approach, and broadening to international partnership and information sharing.

Endnotes

1. *See* Keynote address of Antonio Guterres, secretary-general of the United Nations, at the "High-level Conference on Counter-Terrorism", June 28, 2018 ("[T]he top priority is that we must work together"), https://www.un.org/sg/en/content/sg/speeches/2018-06-28/high-level-conference-counter-terrorism-remarks. *See also* John S. Pistole, assistant director, Counterterrorism Division, Federal Bureau of Investigation, Comments before the Senate Committee on Banking, Housing, and Urban Affairs on September 25, 2003 ("[P]rivate industry and particularly the financial industry… are literally on the 'front lines' in the financial war on terrorism."), https://www.gpo.gov/fdsys/pkg/CHRG-108shrg20396/html/CHRG-108shrg20396.htm.
2. Such informal exchanges include when a bank compliance officer calls a law enforcement agent and makes her aware of a particularly interesting SAR, and when a bank has identified a certain money laundering typology and wishes to brief law enforcement on what the bank is seeing in real time.
3. 31 USC 5318(g)(3).
4. The BSA and operative regulations require financial institutions to disclose documentation supporting the filing of a SAR to federal, state, and local law enforcement agencies, upon request, provided the agencies have jurisdiction over the entity implicated by the SAR. *See* Dept. of the Treasury, FinCEN Advisory, *SAR Confidentiality Reminder for Internal and External Counsel of Financial Institutions* (FIN-2012-A002, March 2, 2012), https://www.fincen.gov/sites/default/files/advisory/FIN-2012-A002.pdf.
5. FinCEN, the U.S.'s FIU, is the central collection agency and repository for 314(a) requests and responses, as well as SARs filed by U.S. financial institutions.
6. Section 314(b), though voluntary, provides financial institutions with the ability to share information with one another for purposes of identifying and, where appropriate, reporting activities that may involve possible terrorist activity or money laundering.
7. In 2017, FinCEN expanded the concept of 314(a) contextual briefings into the FinCEN Exchange. The FinCEN Exchange intends to convene regular briefings – approximately once every six to eight weeks – with law enforcement, FinCEN, and financial institutions to exchange targeted information on priority illicit finance threats. Participation in the programme is strictly voluntary and does not introduce any new regulatory requirements. It is unclear which financial institutions will participate in the FinCEN Exchange, or how those institutions will be selected; it is possible that the programme will be invitation-only, at least in the near term, https://www.fincen.gov/resources/financial-crime-enforcement-network-exchange.
8. https://www.gpo.gov/fdsys/pkg/FR-2017-12-27/pdf/2017-27926.pdf.

9. Nick Kochan, "*How Law enforcement is partnering up with banks in AML fight*", Wolters Kluwer, March 9, 2016, http://www.wolterskluwerfs.com/article/how-law-enforcement-is-partnering-up-with-banks-in-aml-fight.aspx.
10. Established by a handful of senior financial services executives in 2000, the Financial Sector Forum is a membership community of like-minded professionals sharing ideas and knowledge with industry peers. The focus of the members is to improve their understanding of the consumer, the marketplace, and their own marketing performance. What makes the forum unique is that it is independent and sector-specific, and communicates through a mix of events, publications, communities, and online resources.
11. The Home Office is the lead government department for immigration and passports, drug policy, crime, fire, counter-terrorism, and the police, https://www.gov.uk/government/organisations/home-office/about.
12. National Crime Agency, "Joint Money Laundering Intelligence Taskforce (JMLIT)", http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit.
13. *See* U.S. Department of State, Bureau for International Narcotics and Law Enforcement Affairs, International Narcotics Control Strategy Report, Volume II, *Money Laundering and Financial Crimes*, March 2017, https://www.state.gov/documents/organization/268024.pdf. These countries, with the exception of Guinea-Bissau, Haiti, Hong Kong, and Tanzania, also require the reporting of cross-border transactions of currency. Additionally, Bolivia, China, and Iran require the reporting of suspicious transactions, but do not meet other standards.
14. FATF consolidated these recommendations related to information sharing in its publication. *See* FATF 2017 Report. At the time of this writing and per the May 18, 2018, FATF Consolidated Assessment ratings, there remain only four (4) jurisdictions that possess a high rating in those same Immediate Outcomes: Australia (IO2); Spain (IO6); Sweden (IO2); and the U.S. (IO10).
15. FATF 2017 Report at 20.
16. Nick J. Maxwell and David Artingstall, "*The Role of Financial Information-Sharing Partnerships in the Disruption of Crime*", Royal United Services Institute, October 2017 at 15 (RUSI Report), https://rusi.org/sites/default/files/201710_rusi_the_role_of_fisps_in_the_disruption_of_crime_maxwell_artingstall_web_2.pdf.
17. *Ibid.* at 16. *See* also "*Fintel Alliance: Innovation Hub*", produced by AUSTRAC, March 2017.
18. The UK conducted its first national risk assessment in 2015, then again in 2017, to assess the country's ML and TF risk.
19. *See* RUSI Report at 27 and 30.
20. *Ibid.*
21. https://www.fincen.gov/news/news-releases/fincen-launches-fincen-exchange-enhance-public-private-information-sharing.
22. https://www.fincen.gov/resources/fin-exchange/fincen-exchange-frequently-asked-questions.
23. https://www.moneylaunderingwatchblog.com/2017/12/information-sharing-exchange-launched-fincen-improve-suspicious-activity-reporting/. Thus far, information shared at these briefings has helped FinCEN map out and target weapons proliferators, sophisticated global money laundering operations, human trafficking, smuggling rings, corruption, and trade-based money laundering networks.
24. *See* RUSI Report at 16.
25. The Clearing House is a banking association and payments company that is owned by the largest commercial banks and dates to 1853. The Clearing House Association L.L.C. is a nonpartisan organisation that engages in research, analysis, advocacy, and litigation focused on financial regulation that supports a safe, sound, and competitive banking system.
26. *See* "*A New Paradigm: Redesigning the US AML/CTF Framework to Protect National Security and Aid Law Enforcement*", published by The Clearing House, February 2017. (Clearing House Report). Additionally, in October 2009, for instance, the Counter-Terrorism Implementation Task Force (CTITF) of the United Nations recommended that more be done to include the private sector, especially financial institutions, as partners in fighting terrorism financing. Specifically, the CTITF recommended that law enforcement and regulatory authorities "should provide more information and invite more feedback on the implementation, effectiveness, and design of [CTF] measures". *See* CTITF Working Group Report, "*Tackling the Financing of Terrorism*", October 2009, at 10 (Recommendation 32) (CTITF Report). The CTITF further recommended "regular dialogue" be conducted between the public and private sector, to facilitate the design and adoption of appropriate regulation.
27. *See* Clearing House Report. Additionally, the Clearing House recommends revising the AML/CTF supervision structure to have FinCEN claim singular responsibility for large financial institutions. The Clearing House Report argues that only about four banks account for almost half of the total amount of SARs filed to FinCEN, https://www.theclearinghouse.org/~/media/TCH/Documents/TCH%20WEEKLY/2017/20170216_TCH_Report_AML_CTF_Framework_Redesign.pdf.
28. This is also a recommendation from the CTITF. *See* CTITF Report at 9 (Recommendation 28).

Acknowledgment

The authors wish to thank Tracy Angulo, Alexander Warr, Joseph Frenkel, and Ala Shalimava for their assistance.

Appendices

Appendix A – Chart of Countries Requiring Suspicious Transaction Reporting

Appendix A may be found at the following link: https://www.navigant.com/-/media/www/site/insights/gic/2018/business-crime-2019-appendix-a-8-8-18.pdf?utm_source=ICLG&utm_medium=Appendix%20A&utm_campaign=Business-Crime-Guide.

Appendix B – Comparison of Public-Private Partnerships in Six Countries

Appendix B may be found at the following link: https://www.navigant.com/-/media/www/site/insights/gic/2018/business-crime-2019-apx-b-8-8-18.pdf?utm_source=ICLG&utm_medium=Appendix%20B&utm_campaign=Business-Crime-Guide.

Claiborne (Clay) W. Porter
Navigant Consulting, Inc.
1200 19th Street, NW
Suite 700
Washington, DC 20036
United States

Tel: +1 202 973 7211
Email: claiborne.porter@navigant.com
URL: www.navigant.com

Claiborne (Clay) W. Porter is Head of Investigations and a Managing Director in the Global Investigations & Compliance practice at Navigant. Through his supervisory roles and as a Trial Attorney in the United States Department of Justice's Money Laundering and Asset Recovery Section (MLARS), Clay gained extensive experience managing complex, international and domestic financial investigations in matters relating to money laundering, the Bank Secrecy Act (BSA)/AML laws and regulations, U.S. economic sanctions, and anti-corruption and anti-bribery laws.

Professional Experience:

Prior to joining Navigant, Clay held several senior positions in MLARS. As the Acting Principal Deputy Chief of MLARS, Clay supervised the work of approximately 150 attorneys and staff in connection with the various litigating, policy and forfeiture program management units within MLARS. Additionally, he supervised the government's efforts to trace, find, and forfeit the proceeds of high level foreign corruption and prosecute the companies and individuals who launder corruption proceeds. Clay also assisted Departmental and interagency policymakers in developing legislative, regulatory, and policy initiatives to combat global illicit finance, in addition to supervising the DOJ's efforts to find and return forfeited criminal proceeds to victims of crime.

As Chief of the Bank Integrity Unit, Clay supervised the attorneys who were leading the Department's efforts to investigate and prosecute, where warranted, companies and their employees who violate the BSA and U.S. economic sanctions laws and regulations, as well as companies and individuals who launder the proceeds of bribery and corruption. Additionally, Clay interacted on a daily basis with US and foreign law enforcement, bank regulators, OFAC, and FinCEN.

Education:

- Juris Doctorate Tulane: University School of Law.
- Bachelor of Science: Radford University.

Robert Dedman
Navigant Consulting, Inc.
5th Floor, Woolgate Exchange
25 Basinghall Street
London, EC2V 5HA
United Kingdom

Tel: +44 20 7015 8712
Email: robert.dedman@navigant.com
URL: www.navigant.com

Rob Dedman is a Senior Director in Navigant's Global Investigations and Compliance practice in London.

Professional Experience:

Rob joined Navigant from the Bank of England, where from April 2013 he set up the Regulatory Action Division – the Bank of England's enforcement and formal supervisory intervention arm. As Head of that Division, he led the Bank of England's first ever enforcement investigations into misconduct at banks and insurers, achieving significant results against major financial institutions in the UK, and the first ever prohibition of a Chief Executive of a major Bank.

As Head of Division, Rob was the lead adviser on the Prudential Regulation Authority's HBOS Review – a report into the failure of a major UK Bank, and advised Supervisors and Executives (up to Board and Governor level) on significant US criminal and regulatory investigations (including relating to AML, fraud, and anti-bribery and corruption investigations) into major UK financial institutions. He also led the Bank's relationship with enforcers and prosecutors across the globe, including the enforcement relationship with the Financial Conduct Authority, and in relation to investigations carried out by the UK Serious Fraud Office. Rob's role also included advising on the implications (including in relation to privacy) of instances where data held by the regulator had been lost or stolen.

Prior to joining the Bank of England, at the (then) Financial Services Authority, Rob led the legal team responsible for the changes to the UK regulatory system that brought about the creation of the Financial Conduct Authority and the Prudential Regulation Authority.

Education:

- LPC, Legal Practice: The College of Law, Guildford.
- LL.M, UN Law, Law of Armed Conflict, Humanitarian Intervention, EC Competition Law: King's College London.
- Bachelor of Science (Honours), Law and French: University of Surrey.

NAVIGANT

Navigant Consulting, Inc. (NYSE: NCI) is a specialised, global professional services firm that helps clients take control of their future. Navigant's professionals apply deep industry knowledge, substantive technical expertise, and an enterprising approach to help clients build, manage, and/or protect their business interests. With a focus on markets and clients facing transformational change and significant regulatory or legal pressures, the firm primarily serves clients in the healthcare, energy, and financial services industries. Across a range of advisory, consulting, outsourcing, and technology/analytics services, Navigant's practitioners bring sharp insight that pinpoints opportunities and delivers powerful results. More information about Navigant can be found at navigant.com.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com