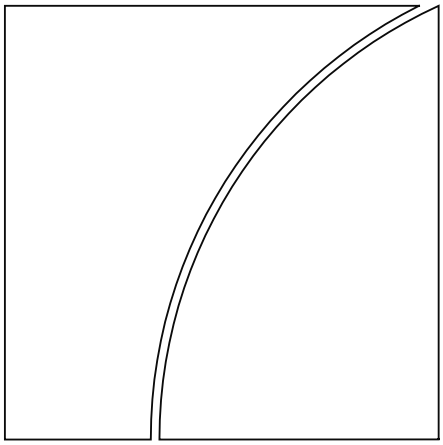
Committee on Payment and Settlement Systems

Board of the International Organization of Securities Commissions



Authorities' access to trade repository data

August 2013

BANK FOR INTERNATIONAL SETTLEMENTS

IOSCO

This publication is available on the BIS website (www.bis.org) and the IOSCO website (www.iosco.org).

ISBN 92-9131-954-6 (print)

ISBN 92-9197-954-6 (online)

Contents

Abbreviations

BIS	Bank for International Settlements
CCP	Central counterparty
CDS	Credit default swap
CPSS	Committee on Payment and Settlement Systems
DMI	Derivatives market intermediaries
DTCC	Depository Trust & Clearing Corporation
FMI	Financial market infrastructure
FSB	Financial Stability Board
IFI	International financial institution
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
LEI	Legal entity identifier
MoU	Memorandum of Understanding
ODRF	OTC Derivatives Regulators' Forum
OTC	Over-the-counter
OTCD	Over-the-counter derivatives
PFMI	CPSS-IOSCO Principles for Financial Market Infrastructures
SIFI	Systemically important financial institution
TIW	Trade information warehouse
TR	Trade repository
WG	Working group
WT	Warehouse Trust Company LLC

1. Foreword and executive summary

1.1 Foreword

In September 2009, the G20 Leaders made a number of commitments regarding the operation of over-the-counter derivatives (OTCD) markets, including the statement that all OTCD contracts should be reported to trade repositories (TRs) in order to improve transparency, mitigate systemic risk and protect against market abuse in the OTC derivatives markets.[1]

A significant amount of attention has been focused on addressing 21 recommendations developed by the Financial Stability Board (FSB) to implement the G20 Leaders statements with respect to OTCD markets, as set forth in its report *Implementing OTC derivatives market reforms* (October 2010).

In October 2011, the FSB advocated that the Committee on Payment and Settlement Systems (CPSS) and the International Organization of Securities Commissions (IOSCO), in co-ordination with relevant authorities, take forward the work on authorities' access to TR data (Recommendation 16),[2] taking into account data security and building on work by the OTC Derivatives Regulators' Forum (ODRF).[3]

A consultative version of this report was published for a comment period that ran from 11 April 2013 to 10 May 2013. During the consultation process, six comments were received, five of which are available on the websites of both IOSCO[4] and the CPSS.[5] The report incorporates relevant comments received during that process.

1.2 Executive summary

TRs are entities that maintain a centralised electronic record (database) of transaction data.[6] TRs will play a key role in increasing transparency in the OTCD markets by improving the availability of data to authorities[7] and the public in a manner that supports the proper handling and use of the data, while taking into account confidentiality requirements.

1 See *Leaders' Statement*, Pittsburgh Summit of the G20 Leaders, 24–25 September 2009, p 9, available at http://www.g20.org/Documents/pittsburgh_summit_leaders_statement_250909.pdf.

2 "Market regulators, central banks, prudential supervisors and resolution authorities must have effective and practical access to the data collected by trade repositories that they require to carry out their respective regulatory mandates. Access to TR information by official international financial institutions also should be permitted in appropriate form where consistent with their mandates."

3 The ODRF, formed in January 2009, brings together representatives from central banks, prudential supervisors, securities regulators and market regulators to discuss issues of common interest, regarding OTC derivatives central counterparties (CCPs) and TRs. The ODRF's scope and focus include information sharing/needs and oversight coordination and cooperation. It is not a standard-setting body and does not provide guidance on interpreting standards. The ODRF's work is intended to complement the mandates, responsibilities and focus of other international committees and groups that bring together public authorities and their efforts. See http://www.otcdrf.org/documents/scope_relationships_mar2010.pdf.

4 http://www.iosco.org/library/index.cfm?section=pubdocs&publicDocID=408

5 http://www.bis.org/publ/cpss108/comments.htm

6 CPSS-IOSCO *Principles for financial market infrastructures*, p 9, available at www.bis.org/publ/cpss101a.pdf and http://www.iosco.org/library/pubdocs/pdf/IOSCOPD377.pdf.

7 The term "authorities" is intended to encompass at a minimum public sector authorities including central banks, securities and market regulators, prudential supervisors of market participants, resolution authorities and other authorities that would have a material interest in OTC derivatives data in furtherance of a regulatory mandate or legal responsibilities. In some instances, law enforcement authorities may also have a legal right to access data from TRs. The term authorities under this

The aim of this report is to provide guidance to TRs and authorities on access to TR-held OTCD transaction data,[8] as well as possible approaches to addressing confidentiality concerns and access constraints. This report describes the expected data access needs of authorities using a functional approach complemented by an illustrative data access mapping that aligns each function to the minimum level of access authorities would typically require in support of their mandates and responsibilities.[9] This report recalls that previous international initiatives have already set out useful recommendations and principles addressed to authorities and TRs to provide a basis for promoting effective and practical access to data maintained in TRs for all relevant authorities. The CPSS/IOSCO *Principles for financial market infrastructures* (PFMI), particularly Principle 24 on disclosure of market data by trade repositories and Responsibility E on cooperation with other authorities, are useful in this context as well as Recommendation 16 of the FSB report on *Implementing OTC derivatives market reforms*. Drawing on these principles, responsibilities and recommendations, the report proposes access guidelines that aim to provide TRs and regulators with a framework upon which to build access policies. The data access mapping table provides a means for mapping access rationales to access levels. Authorities and TRs are encouraged to develop and maintain access policies and arrangements informed by the guidance and mapping outlined in this report.

It is likely that OTCD data will be held in multiple TRs, requiring some form of aggregation of data to get a comprehensive and accurate view of the OTC derivatives market and activity globally. With the current structure of TRs, no authority will be able to examine the entire global network of OTCD data at a detailed level.[10] In the light of this limitation, the public sector may wish to consider and further investigate the opportunity and feasibility for a centralised or other mechanism to produce and share global aggregated data, as a complement to the direct access by the different authorities to TR-held data. Outlining such an arrangement is beyond the scope of this report but will be addressed by a feasibility study mandated by the FSB on approaches to aggregate OTC derivatives data.

The guidance set out in this report should not be seen as preventing an individual authority from obtaining data for which it has the authority to obtain directly from a given TR based on its mandate.

report is therefore wider than the legal definition of an authority in a given jurisdiction's provisions on legal powers and enforcement.

[8] The G20 statement which is referred to above relates only to OTC derivatives. Nevertheless, in some jurisdictions, the scope of products reported to TRs is broader (eg the EMIR Regulation in the European Union is mandating the reporting of exchange traded derivatives to TRs). This report is focusing on OTC derivatives and the definition of typical data requests with respect to the functional mandates applies accordingly only to OTC derivatives trades. However, the framework and access guidelines proposed by the report could also be relevant for other types of transactions that could be reported to TRs, including exchange-traded derivatives.

[9] In describing levels of access that authorities would typically require, this report does not intend to imply that each authority requesting data under a given mandate would necessarily request all the data available to them as described in Section 3 and in the data mapping table.

[10] Another obstacle to the possibility of examining the global network of OTCD data is the insufficient technical standardisation of data reporting fields and formats, which adds complexity to the aggregation of data. This issue was addressed in the CPSS/IOSCO report of January 2012 on OTC derivatives data reporting and aggregation requirements. In order to facilitate data aggregation, follow-up international initiatives, such as the implementation of the LEI (Legal Entity Identifier), are currently under way, which the present report acknowledges as being critical. Further work on standardisation, based on comments received through the consultation period, will be considered especially by a feasibility study mandated by the FSB on approaches to aggregate OTC derivatives data.

2 Introduction

2.1 The role of TRs in maintaining data and improving transparency

The recent financial crisis highlighted a severe lack of transparency in the OTCD markets. The lack of available data during the crisis hindered authorities in effectively carrying out their mandates. It also interfered with the assessment of risks resulting from the build-up of unsustainable exposures, which ultimately led to the collapse or near-collapse of some major financial institutions. Increased transparency may improve the stability of these markets by enhancing the ability of authorities to monitor and detect risks.

TRs have emerged as a new type of FMI and have grown in importance as a key component of the infrastructure supporting OTCD markets. By centralising the collection, storage and dissemination of transaction data, a well designed TR that operates with effective risk controls can serve an important role in enhancing the transparency of transaction information to relevant authorities and the public, promoting financial stability, and supporting the detection and prevention of market abuse. TRs may also play an important role in standardising and normalising the representation of OTCD transactions across a critical mass of market participants and consequently allowing for otherwise unavailable systemic views of the OTCD markets.

As a consequence, legislative and regulatory efforts are underway to implement in the G20 jurisdictions the commitment to report OTCD transactions to TRs.

Although the development of TRs began in the mid-2000s, they are still a relatively new type of FMI. In recent years, significant developments have occurred in this area and are still ongoing. The G20 commitments to improve transparency in OTCD markets are expected to increase the importance of TRs within the global architecture of financial markets stability.

2.2 Background work on TRs

Substantial work has already been carried out in implementing the G20 commitment to report OTCD transactions to TRs, and in ensuring consistent access to these data by the regulatory community. This report on authorities' access to trade repository data draws on these previous efforts as a basis for furthering the G20 commitment.

The ODRF had considered a number of issues related to OTCD data in its discussions. Two workstreams are particularly relevant to authorities' access to data. First, in June 2010, the ODRF developed indicative guidance to Warehouse Trust (WT) aiming to identify data that authorities would expect to request from WT (Warehouse Trust Guidance) to carry out their mandates.[11] The Warehouse Trust Guidance consisted of suggested high-level principles as well as a corresponding table that mapped the potential credit derivatives data requests that various authorities were likely to submit to the TR in connection with their responsibilities; the table was provided as a reference for WT when responding to requests from authorities. WT voluntarily incorporated the Warehouse Trust Guidance into its operational procedures for responding to data requests from various authorities.

Following on from this work, a subgroup of the ODRF members also conducted some preparatory work to develop a more comprehensive framework that took into account authorities' access to data maintained in TRs more broadly. This work elaborated on the levels of access that

[11] The Warehouse Trust Company LLC is a subsidiary of DTCC Deriv/SERV LLC. For the first half of 2012, WT operated DTCC's Trade Information Warehouse, which provides a centralised electronic trade database for OTC credit derivatives contracts. This functionality was subsequently transferred to DTCC's Derivatives Repository Ltd, located in London.

different types of authorities would typically require. Although this work was not pursued by the ODRF, it was provided to CPSS and IOSCO to inform this report.

Additionally, CPSS and IOSCO have taken significant steps towards defining requirements regarding data to be reported to TRs and aggregation of that data.[12] The Data Report made recommendations for minimum data reporting requirements and potential methodology and mechanisms for data aggregation on a global basis.

The PFMI introduced a specific principle for TRs that places emphasis on the need to disclose TR-held data to relevant authorities in line with authorities' respective mandates or responsibilities.[13]

In addition to the above mentioned workstreams, this report is informed by practical lessons drawn from authorities' recent experiences with respect to data requests under the Warehouse Trust Guidance. Although these experiences show the utility of the Warehouse Trust Guidance, this report identifies and addresses certain limitations in that guidance. The Warehouse Trust Guidance was drafted at a time when there was only one operational TR and it specifically addressed authorities' needs for data on credit derivatives. The number of TRs has since increased, and TRs now hold data for transactions in several asset classes. In addition, the Warehouse Trust Guidance was prepared in a context where most legislation regarding OTCD and TRs was still under consideration, and even now many jurisdictions are still developing or finalising legislation or subsidiary rules. A key lesson learned is that, in order for TRs to meet the data needs of various authorities, they should benefit from guidance regarding expected access needs from such authorities. TRs would also benefit from guidance with respect to access needs that span OTCD classes, to help ensure consistency across TRs.

2.3 Rationale for providing guidance for authorities' access to TR data

In connection with the G20 commitment on OTCD data reporting, authorities must have effective and practical access to the OTCD data they require to carry out their respective mandates. The ability to access OTCD data held in TRs represents a significant change from the methods that authorities have traditionally used to access information related to OTCD transactions. Access to TR data will enable authorities to move from decentralised access to information (directly from reporting entities or from each other) to more centralised access (through TRs that collect and store data from reporting entities and facilitate access by authorities to that data). In this respect, greater use of TRs could improve the efficiency and effectiveness of authorities in performing their mandates.

An increasing number of jurisdictions have implemented or are in the process of implementing the G20 commitment on OTCD data reporting in their legal and regulatory framework. As a consequence, certain data requests from an authority for data stored in a TR may be based upon a legal right for an authority in its jurisdiction to require the TR to provide data, irrespective of the TR's primary regulator or location. Furthermore, the TR may be obligated to comply with such data requests as a condition for the recognition or eligibility of the TR in the authority's jurisdiction to act as a TR in furtherance of trade reporting requirements. Accordingly, a TR may be required under law or regulation to provide data requested pursuant to the mandate of the requesting authority.

At the same time, the centralised storage of OTCD data also underscores the importance of confidentiality constraints on the handling of market participant data. The confidentiality of information provided by reporting entities directly to authorities has typically been protected by statute or regulation that restricts its use and dissemination. TRs will very likely store information that would typically be entitled to confidentiality protection if reported directly to an authority with legal jurisdiction over the

[12] CPSS-IOSCO *Report on OTC derivatives data reporting and aggregation requirements*, January 2012 (Data Report).

[13] See CPSS-IOSCO PFMIs, Principle 24.

participant or the transaction.[14] Issues of confidentiality gain importance as the circle of authorities requesting access to TR data expands. In this context, it is essential to provide guidance and safeguards that will address these confidentiality concerns yet still help ensure that authorities have access to the relevant information needed to carry out their respective mandates.

Without guidance on authorities' typical access needs and confidentiality safeguards, some authorities may be reluctant to allow counterparties within their jurisdiction to report to TRs outside their jurisdiction with the consequence that it may prompt requesting authorities to require the establishment of TRs in their jurisdiction to avoid such obstacles. Clear guidance is helpful in ensuring that such confidentiality concerns do not serve as the sole motivation to establish a TR where no independent business reason exists for such an entity. The multiplication of TRs for the same OTCD class may actually increase the operational complexity for authorities in obtaining effective and practical access to information.

In the light of the foregoing, the guidance set out in this report regarding the scope of data access should not be taken as definitive. As noted above, the data mapping table for each mandate describes the minimum level of access that an authority exercising that mandate would typically require. Additionally, the needs of authorities will probably continue to evolve, and authorities may find that the descriptions of their respective mandates do not adequately describe the full range of their data access needs. Given the continuous evolution of the OTCD markets, TRs will need to develop data access procedures that are sufficiently flexible along different dimensions, including the composition of typical data requests and reported attributes for specific OTCD classes. The framework and guidelines outlined in Section 5 should provide useful guidance in making and responding to such requests and the implementation of data access policies by TRs.

2.4 Addressees and scope of the report

The guidance set out in this report is addressed to both authorities and TRs. The report is addressed to authorities to encourage a common understanding within the official sector and facilitate mutual support of authorities' respective access needs in support of the expectations set out in Responsibility E of the CPSS-IOSCO PFMI; for TRs, it provides guidance on the implementation of Principle 24 of the CPSS-IOSCO PFMI.

This report follows a functional approach that describes typical access needs with reference to the mandate(s) that authorities are responsible for carrying out and would need data to support. Under this functional approach, a mandate is considered with respect to its particular objective, addressees or perspective in contrast to an institutional approach, which would look at the type of authority that performs the mandate. The functional approach recognises that some authorities may perform several functional mandates and that these mandates may be combined in various ways depending on the legal framework of the different countries. This report does not prescribe nor recommend any specific structure for the institutional framework in a particular geographic territory.

These mandates include (but are not necessarily limited to) the following:

- Assessing systemic risk including:
  - Examining size, concentration, interconnectedness and structure of markets and institutions, from the perspectives of both macro systemic risk and micro systemic risk;
  - Evaluating derivatives for mandatory clearing determinations and monitoring compliance with such determinations;

[14] For the purpose of this report and unless "legal jurisdiction" is explicitly mentioned, jurisdiction refers to the geographical territory of a public authority and not to the particular legal scope of the mandate, which scope could extend to different countries or regions.

    - Evaluating derivatives for mandatory trading determinations and monitoring compliance with such determinations.
- Performing general macro assessment.
- Conducting market surveillance and enforcement:

  This includes conducting market surveillance of trading activities and enforcement of charges against unlawful trading activities.
- Supervising market participants, comprising authorities in charge of:
    - Registering market participants (eg dealing or trading entities);
    - Supervising market participants with respect to business conduct and compliance with regulatory requirements; and
    - Prudentially supervising financial institutions.
- Regulating, supervising or overseeing trading venues and FMIs, including:
    - exchanges, organised markets or organised trading platforms;[15]
    - payment or settlement systems;
    - CCPs; and
    - TRs.
- Planning and conducting resolution activities:

  This includes pre-resolution planning activities and coordinating resolution activities across jurisdictions.
- Implementing currency and monetary policy, and lender of last resort:
    - Managing currency policy;
    - Implementing monetary policy; and
    - Acting as the lender of last resort.
- Conducting research to support the above functions.

It is important to note, however, that authorities with other mandates not listed here or discussed below may have an interest in and a mandate that would support their access to data stored in TRs. Therefore, the above list should not be viewed as complete or exclusive.[16]

In line with Recommendation 16 of the FSB report on *Implementing OTCD market reforms*, this report will consider issues pertaining to access of international financial institutions (IFIs) to TR-held data.

This report also addresses how authorities could mutually support each other in their respective access to relevant data, which is consistent with the PFMI's Key Consideration 8 of Responsibility E on cooperation with other authorities. Key Consideration 8 states that "Relevant authorities should coordinate to ensure timely access to trade data recorded in a TR".[17]

[15] Including supervision of listing rules.

[16] TRs should ensure that authorities with mandates not discussed in this report have access to TR data commensurate with their mandate(s). In determining what level of access is appropriate for a given mandate, TRs should give due consideration to the supporting recommendations and guidelines outlined in Section 5.

[17] The Data Report has already addressed issues relating to the frequency of TR data access and the methods of TR data disclosure.

2.5 Organisation of the report

The report first summarises the various functions and corresponding data needs of authorities (Section 3) and then delineates approaches to facilitating appropriate and effective access to TR data (Section 4).

The guidance is provided in Section 5, which sets forth the framework and guidelines for authorities' access to TR data, and Section 6, which reflects the data access mapping.

3 Authorities' data needs

3.1 General approach and definition of the different access levels

3.1.1 General approach

Building upon the Data Report, which recognised that authorities have varied data needs that may evolve over time according to their respective mandates, this section aims at identifying the typical data access needs associated with each of the different functional mandates carried out by authorities.[18] Rather than focusing on the various institutional types of authorities that may have mandates which touch upon the OTCD markets, this section adopts the functional approach described in the FSB's Recommendation 16, analysing the function of each mandate in the financial market and the type of access required to enable authorities to carry out this function.[19]

The purpose of this report is to address the minimum level of detail that an authority accessing TR data would typically require in order to fulfil its mandates, whether or not the data records contain each of the data elements or fields that the authority seeks. Requesting authorities should consider the restrictions of data availability. Thus, it is possible that a TR may not contain in its records particular data elements or fields sought by one or more types of authority (for example, because they are not required to be reported by that entity's authority).

The discussion that follows is not intended to prescribe how authorities carry out their mandates but rather is meant to illustrate why authorities may need varying levels of access to TR data to carry out their mandates. Some jurisdictions have a long tradition of financial industry self-regulation, through the delegation of regulatory mandates to FMIs or organisations. This report does not directly address the data access needs of self-regulatory organisations (SROs) that perform specific mandates pursuant to statutory delegation of authority and which may require access to data to fulfil these mandates.[20] The determination of data access arrangements that should apply to such organisations

[18] We note that this report addresses data access needs. The issue of data needs or gaps, which involve identifying particular data elements or fields that participants should be required to report into a TR or that an authority may require to fulfil its mandates, is beyond the remit of this working group.

The FSB set up the OTC Derivatives Data Experts Group (ODEG) in February 2012 to outline the types of OTCD-related data that would assist the official sector in assessing systemic risk, supervising market participants and conducting resolution activities. See *OTC Derivatives Markets Reform, Third Progress Report on Implementation*, FSB, 15 June 2012, p 24, http://www.financialstabilityboard.org/publications/r_120615.pdf.

[19] This section focuses on those mandates that are currently understood to require OTCD data for their effective execution. The mandates discussed herein are not intended to be exclusive; to the extent that an authority has a mandate not included in this section for which it requires access to TR data, TRs and TR supervisors should consider a request for access pursuant to that mandate in the light of the general principles articulated in Section 5.

[20] Because self-regulation takes a variety of forms, it is appropriate to distinguish between voluntary or autonomous self-regulation and compulsory self-regulation based on a mandate or a statutory delegation of authority. Voluntary or autonomous self-regulation is based solely on private autonomy and is, by definition, established without any government involvement (examples include codes of conduct issued by professional associations). Compulsory self-regulation is based on

requesting data held in TRs should be left to the supervising authority of that organisation. Supervised organisations performing mandates pursuant to statutorily delegated authority may have different roles and responsibilities, and the legislation governing such delegation can vary significantly from one jurisdiction to another.

However, such supervised organisations would typically need to request data as part of their efforts to fulfil their mandate. Such organisations with an official mandate would typically require access commensurate with their mandate. As they are not public authorities per se, it is important that the TR be able to identify the specific nature of the mandate of such organisations and to distinguish requests based on that mandate from requests motivated by a commercial interest in data that would not entitle the organisation to the same level of access as would be appropriate for a public authority. Moreover, we note that a supervised organisation should not have access greater than the access of its supervising authority pursuant to that authority's own mandate(s). In other words, the access rights to TR data by the organisation should never be superior to its supervisory authority's access rights to TR data pursuant to the same mandate. These organisations should also be subject, at a minimum, to the same constraints as the authority(ies) supervising them, especially for confidentiality and organisational requirements.

3.1.2 Description of different access levels

Data stored in TRs can serve authorities in several ways. Typical access needs for each function can be described along three separate dimensions, which reflect differing levels of detail in which TR data can be aggregated and presented: depth, breadth and identity.

Depth specifies one of three basic levels of detail describing the granularity of authorities' access to TR data needed to fulfil their mandate(s): transaction-level, position-level, or aggregate-level.[21]

Transaction-level refers to the depth at which an authority may view data that are specific to uniquely identifiable participants and transactions.[22] A transaction represents a single economic relationship between two counterparties, defined by a contract. A transaction record typically specifies (a) the contract terms and (b) both counterparties to the contract.

Position-level refers to the depth at which an authority may view data reflecting both the gross and netted open positions that are specific to (a) a uniquely identifiable participant or (b) for a particular OTCD product or class (a set of transactions pertinent to a pair of participants). Position-level data are a snapshot at a point in time of all open positions for a particular product or type of products or for a given counterparty or group of counterparties. Unlike transaction-level data, this aggregation level does not include data reflecting the details of individual transactions, but the summing of one or more transactions will provide position information for one or more counterparties at a point in time.

Aggregate-level refers to the depth at which an authority may view both gross and netted data attributable to all participants that may be summed using various categories, including by product, currency, region, underlier etc that are not specific to any uniquely identifiable participant or

a mandate from statutory delegation of authority to require that a given regulatory function be addressed through self-regulation.

[21] Consistent with the Data Report, authorities will need a detailed understanding of the methodology used by the TR to calculate values for aggregation for position-level and aggregate-level data, when this task is performed by the TR. In many cases, successful analysis requires multiple levels of aggregation to be spanned, and regulators need to understand how a position was created. Note that access to more granular information should not prevent an authority from also having access to aggregated information based on the more granular information (for example, access to transaction-level information should also allow for position-level and aggregate-level information based on this information).

[22] Transaction-level data can reflect either stock (transactions that represent all open interest for a particular participant or underlier at a given point in time) or flow (transactions, whether involving currently open interest or not, over a defined time interval). Transaction-level access would enable an authority to view either stock or flow data for the relevant transactions.

transaction.[23] This is also the level of detail to which the public could have access. Some TRs already make aggregate-level data available to the public.

Example of access levels

Type of data	Depth	Examples
Transaction-level data	Open transaction record	Full details of individual transaction status records. A single name five-year CDS between Bank X and Bank Y where Bank X buys from Bank Y USD 100m notional protection on underlier[24] ABC and collateralised by X.
Position-level data	Counterparty	Gross notional amount outstanding of Bank X's open buy positions in underlier ABC.
Aggregate-level data	Aggregate	Gross notional amount outstanding for underlier ABC.

Breadth specifies the access to data, at the varying levels of depth defined above, that an authority will typically need to fulfil its mandate, described in terms of participants or underliers. Breadth may extend from all participants or underliers worldwide to a more limited range, such as those under its authority.

Identity refers to whether the reported data identifies counterparty information (at the transaction or position level) or contains only anonymised data and, if anonymised, whether it contains any identifiers that would allow unique participants to be separately identified.[25] An anonymised counterparty may be given a unique identifier that is not a name (eg an ID number that does not allow the identification of the counterparties).

3.2 Authorities' functional mandates

The following section will describe in a stylised way the different functional mandates of authorities and the associated data needs, with respect to OTCD stored in TRs. The detailed mapping in Section 6 will

[23] Participants generally refer to counterparties to OTCD transactions and may include entities that are directly regulated or supervised by the authority and entities that are not directly regulated or supervised by the authority but participate in markets that it regulates.

A transaction record typically specifies an underlier whose measurable performance governs the value of the transaction. For purposes of access policies, most underliers can be placed in a few categories: some transactions reference underliers that involve cash instruments (eg debt or equity securities), including baskets of securities (which baskets may be custom and standardised and would include index and indices); other transactions reference underliers that involve listed derivatives instruments (ie futures or exchange-traded options); also, a large number of transactions reference underliers that do not involve a financial instrument but instead involve a measurable variable, such as an interest rate, a foreign exchange rate, or a commodity price.

[24] In this example, the underlier is a reference entity that can be broken down at a granular product level, such as IRS data, which should be available by underlying index (eg LIBOR), maturity etc.

[25] Identification of participants will be facilitated by the use of legal entity identifiers (LEI). "Minimum reference or identification data associated with a LEI would include the information needed to identify, on a verifiable basis, the legal entity holding a LEI, such as its place of incorporation, the address of its corporate headquarters and its ultimate parent company." CPSS-IOSCO Data Report, p 29.

The FSB published a report that lists a set of reference data attributes regarded as the minimum set of information that should be available at the launch of the LEI. See FSB, *A global legal entity identifier for financial markets*, 8 June 2012.

complement this description in summarising the expected minimum access levels for each type of functional mandate.

3.2.1 Assessing systemic risk

Systemic risk refers to the potential that an event, action or series of events or actions will have a widespread adverse effect on the financial system and, in consequence, on the economy. Authorities with systemic risk mandates are concerned about systemic risk because it not only has the potential to harm a large number of investors and market participants, but because it also can have a widespread negative effect on financial markets and the economy.

From a structural point of view, mandates linked to systemic risk may be differentiated according to their macro and micro orientation. On the one hand, macroprudential supervisors may be responsible for the macroprudential oversight of the financial system mitigating systemic risks to financial stability that might arise from developments within the financial system and taking into account macroeconomic developments. On the other hand, microprudential supervisors may be statutorily obligated to review and respond adequately to the systemic risk they identify in the scope of their mandate(s). Proper coordination between both levels typically exists, so as to facilitate the interchange and standardisation of information, avoid the duplication of tasks and fully exploit the expertise of the authorities in their respective fields.

For the purpose of identifying potential areas of systemic risk, authorities will need to understand aspects that relate to market participants, market characteristics and the infrastructure of the OTCD markets. For example, authorities can use OTCD data to assess trends and concentration levels in markets, and to monitor the positions of individual institutions that could cause wider disruptions in the financial system due to their size, common exposures to particular risk factors or interconnectedness (see eg FSB-IMF-BIS (2009)).TR data would help them assess whether the failure of such participants could transmit severe shocks to other participants.

TR data should facilitate authorities' systemic risk analysis by providing information that can be used to study size, concentration, interconnectedness and structure with respect to institutions (including systemically important financial institutions (SIFIs) and systemically important financial markets and infrastructures). The precise data requirements are likely to depend on the particular question at hand, and may also differ across authorities.

For each of the areas of systemic risk analysis, the three data dimensions addressed in Section 3.1 will be considered: depth, breadth and identity.

3.2.1.1. Opportunity for a centralised or other mechanism to collect and share global aggregated data

With the current structure of TRs, no authority will be able to examine the entire global network of OTCD data at a detailed level. In addition, it is likely that OTCD data will be held in multiple TRs, requiring some form of aggregation of data to get a comprehensive and accurate view of the global OTC derivatives market and activities. Absent that, the G20's financial stability objectives in calling for TRs might not be achieved.

In the light of these limitations, the opportunity for a centralised or other mechanism to provide global aggregated data, as a complement to the direct access by the different authorities to TR-held data, probably warrants consideration and further investigation, although beyond the scope of this

report.[26] This will be addressed by a feasibility study mandated by the FSB on approaches to aggregate OTC derivatives data.

3.2.1.2. Examining size

Size refers to the scale of activity (eg volumes) or positions (eg outstanding notional or mark-to-market amounts) in a defined population. Financial institutions with large notional or mark-to-market amounts or volumes may pose greater scope for systemic disruptions, ceteris paribus, than similar institutions with smaller notional or mark-to-market amounts and volumes when trading in the same OTCD classes.[27] TR data can also provide insight into positions built up by one or more entities that may include SIFIs. For example, authorities may wish to be aware of the size of exposures built up by SIFIs in their legal jurisdiction to a particular sector that is considered vulnerable.

Size is the area that may require the least level of data detail. In terms of depth, it may be sufficient to have aggregated data, but broken down to a level of sufficient detail to make the aggregation meaningful. A minimum would be the OTCD class, product type, underlying risk type, currency denomination, origin country of underlier and counterparties, and maturity.

As for breadth, given the global nature of the OTCD markets, authorities would typically have an interest in seeing trends in aggregate growth in the market as a whole, as opposed to trends in just one country (eg growth in CDS on sovereigns globally). If the banking sector as a whole in country X has an exposure to a bank, or to the banking sector as a whole, from country Y, then the authority from country X may want to be able to measure that exposure.

Since the data are aggregated, counterparty identities are typically not needed, but it might be useful to know the main characteristics of the counterparties (eg dealer or non-dealer) and of the underliers, such as their sector and country.

3.2.1.3. Examining concentration

Concentration refers to the relative role of individuals or groups of financial institutions within a market segment. The build-up of relatively large volumes of activity or relatively large positions (as measured by notional or mark-to-market amounts outstanding) in some defined population could increase systemic risk.

In terms of depth, authorities may want to see position-level data. Additionally, some high-level questions can be answered using aggregate data (eg on the relative weight of particular reference entities within a market segment for CDS contracts). But authorities may wish to see position-level data to analyse the concentration of exposures among the institutions holding the relevant OTCD positions.

Aggregate data, which lack information on bilateral relationships or identities of the counterparties, are only useful when analysing the concentration of positions by underlier, but they do not reveal who holds those positions. Authorities may also need position-level data to answer any questions on concentration of exposures among financial institutions, both to (i) counterparties and to (ii) reference entities in the case of CDS.

[26] For performing macro assessments, or supporting provision of data for systemic risk analysis, it is probably worth investigating the feasibility of how a centralised or other mechanism would be able to collect position-level and transaction-level data from TRs globally and aggregate, summarise and ensure anonymity of the data, subject to applicable local law. The data's granularity could entail breakdowns by jurisdictions and counterparty types.

Such a mechanism could support making the data available to all relevant authorities in regular standardised reports that would parallel and complement, for example, the international financial statistics or the OTCD survey data. It could also facilitate publication of a set of aggregate data.

[27] For example, a wave of defaults in a particular corporate sector could have a significant impact on a country's financial sector if its banks had sold a large number of CDS contracts written on that sector. TR data are of use here as they allow authorities to take stock of current positions and to monitor growth trends.

Regarding the breadth of data needed, an authority may have an interest in data for counterparties and underliers within its legal jurisdiction. An authority may have an interest in data for all market participants (and, in the case of CDS, reference entities) globally.

Finally, the identity may be needed for the analysis of certain issues. An authority interested in examining the relative concentration of exposures of a particular entity in a particular market segment will need named data. In contrast, if one was interested in a more abstract analysis of market concentration (eg to understand the market's reliance on a few key participants), then anonymised data would suffice. For anonymised data to be useful when examining concentration, all counterparties and reference entities need to be individually and uniquely identified by a code.

3.2.1.4. Examining interconnectedness

Interconnectedness refers to the nature, scale and scope of obligations that arise between and among institutions. Analysis of interconnectedness involves describing and analysing the network of links across participants within a segment of the OTCD market, and/or across different segments. It shows who the central players are, where the vulnerable links are and how the shape and characteristics of the network change over time. Analysis of the network complements the information on concentration, and underpins the assessment of how far market participants are exposed to common shocks. Understanding interconnectedness is crucial for assessing the likelihood and extent of contagion in the financial system. For example, it may help to signal the potential for so-called liquidity spirals, where margin calls in one market segment may affect financial institutions liquidity needs in other, related markets.

To analyse interconnectedness, authorities would need to be able to construct a complete network of exposures or positions (including but not limited to OTCD data). As in the case of concentration analysis, authorities would require position-level data in terms of depth.

In terms of breadth, authorities would typically require data for counterparties and underliers within its legal jurisdiction. An authority may also have an interest in all institutions globally and all underliers regardless of the country of origin, given the global nature of the exposures.

The functional utility of network analysis is greatly enhanced if the identity of each counterparty (which can nonetheless be anonymised if necessary) is included. To conduct network analysis and make use of the robust set of mathematical tools it provides, the data requested at the transaction-level information should be organised by unique counterparty, by underlier and by the direction of the trade. It could also be useful to know the domicile of both counterparties and to identify the importance of certain critical "nodes", that is, the country and sector of each counterparty (identity can nonetheless be anonymised if necessary) may be needed.

3.2.1.5. Examining structure

A disruption in an area of the market that supports financial activity such as trade or post-trade infrastructure can be a significant source of systemic risk, both for financial institutions who rely on these markets for their funding and risk management activities, and for other, related financial markets. Sound market infrastructure policy, to the extent practicable, should be informed by data on the underlying market structure. It follows that a well functioning market needs a robust structure (pre-trade and post-trade) supported by liquidity providers such as large global dealers.

A high level of detail would be needed to analyse the structure of markets. Here the depth provided by transaction-level data would be necessary. Monitoring changes in the total trading volumes, the trading frequency or the role of certain liquidity providers could alert authorities to potential changes in liquidity in those markets and to changes in their systemic importance that might call for market structure changes.

In terms of breadth, data on all counterparties globally would typically be needed, as the aim is to understand the structure of the market as a whole. This insight could not be gained if the authority

only had access to data on the institutions operating within its own legal jurisdiction, which is the current status in most, if not all, jurisdictions where cooperation arrangements are required for data transfer.

Anonymised data where counterparties are uniquely identified and additional information such as sector and country is provided[28] might allow for a general understanding of liquidity provision, as well as of how and whether liquidity varies across time.

An authority in charge of a systemic risk mandate (examining size, concentration, interconnectedness, structure) should have access to named transaction-level data for institutions and underliers in its legal jurisdiction. It should also have access to anonymised transaction-level data for all market participants globally.

3.2.1.6. Evaluating derivatives for mandatory clearing determinations and monitoring compliance with such determinations

The G20 commitment provides that all standardised OTCD contracts should be cleared through CCPs. Some jurisdictions have established or will be imposing mandatory clearing requirements. TRs will be an important source of information regarding OTCD that are not centrally cleared as data gathered from TRs will not only assist authorities in determining which OTCD will be suitable for mandatory clearing, but will also assist authorities in monitoring its implementation.

TR data could allow authorities to track progress in the take-up of standardised OTCD products and assess the proportion of those contracts that are being centrally cleared. The increased use of CCPs is a core part of the G20 OTCD reform programme. To support this commitment, many jurisdictions have or are imposing mandatory clearing in legislation and rules. These often include a bottom-up approach, where CCPs submit derivatives or classes of derivatives to authorities who then will determine if such derivatives should be subject to a central counterparty clearing obligation. They may include a top-down approach where authorities review derivatives information from other sources to make such determinations. TRs will be an important source of information to help authorities with mandatory central clearing determinations, for example, by allowing them to measure available liquidity and product standardisation more generally, and by assisting authorities in identifying potential new clearable contracts to require to be cleared.

To make an informed decision on whether a product should be subject to a clearing requirement (and any type of exception to a clearing requirement), an authority will need, amongst other things, to analyse the liquidity of products referencing underliers within its legal jurisdiction or traded by participants within its legal jurisdiction, as well as how the product is traded, the degree of standardisation of the product's contractual terms and operational processes, and the availability of fair and reliable and generally accepted pricing sources.[29] This analysis will typically require not only the positional data (gross and net notionals), but also the number and type of different counterparties to a product over a particular timeframe, the number of transactions over that timeframe, the cumulative notional traded over that timeframe, and the distribution of transaction volumes over that timeframe. Authorities will therefore typically require access to detailed information regarding the transaction and its economic terms, as well as aggregated information regarding volumes, notional and mark-to-market values and the number and type of counterparties who trade the OTCD. Authorities may also require access to information on transactions involving the same type of OTCD contract as the one being evaluated, whether or not the counterparties or underliers are in the authorities' legal jurisdiction.

[28] For instance, a useful reference may be the BIS sector classification for interbank statistics, available at http://www.bis.org/statistics/intfinstatsguide.pdf.

[29] See IOSCO Technical Committee, *Requirements for Mandatory Clearing*, February 2012, p 16, available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD374.pdf. See also, FSB report, *Implementing OTC Derivatives Market Reforms*, October 2010, p 4, available at http://www.financialstabilityboard.org/publications/r_101025.pdf.

As for breadth, based on these needs, an authority with a mandate to evaluate OTCD for mandatory clearing determinations will typically have an interest in transaction-level data for transactions involving either underliers within its legal jurisdiction or participants within its legal jurisdiction. Identities and names may not be required, as anonymised counterparty information may be sufficient, but even with anonymised data, the country identifier of the counterparties and the currency identifier of the transactions should be relevant in this analysis. However, authorities may require access to named data in order to understand the impact of mandatory clearing determinations on market participants as well as to monitor the compliance with such requirements by market participants.

3.2.1.7. Evaluating derivatives for mandatory trading determinations and monitoring compliance with such determinations

The G20 commitment provides that, where appropriate, all standardised OTCD contracts should be traded on exchanges or electronic trading platforms ("organised trading platforms"). Some jurisdictions have established or will be imposing mandatory trading requirements. TRs will be an important source of information regarding OTCD that are not trading on organised trading platforms and can potentially act as centralised collection points for trading activity data from organised trading platforms, thus allowing authorities to better characterise trading liquidity.

To make an informed decision on whether a product should be subject to a trading requirement (and any block or other type of exception to the latter), authorities will need to analyse the liquidity of products referencing underliers or traded by participants within their legal jurisdictions, as well as other relevant factors about the product. This analysis will typically require not only the positional data (gross and net notionals), but also the number of different counterparties to a product over a particular time frame, the number of transactions over that time frame, the cumulative notional traded over that time frame, and the distribution of transaction volume over that time frame. Authorities will therefore typically require access to detailed information regarding the transaction and its economic terms, as well as aggregated information regarding volumes, notional and mark-to-market values and the number of counterparties who trade the OTC derivatives.

As for breadth, based on these needs, an authority with a mandate to evaluate OTCD for mandatory trading determinations will typically have an interest in transaction-level data for transactions involving either underliers within its legal jurisdiction or participants within its legal jurisdiction. In some cases, data for underliers outside an authority's legal jurisdiction may be required to determine the systemic importance of such underliers.

Identities and names may not be required, as anonymised counterparty information may be sufficient, but even with anonymised data, the country identifier of the counterparties and the currency identifier of the transactions should be relevant in this analysis. However, authorities may require access to named data in order to understand the impact of mandatory trading determinations on market participants as well as to monitor the compliance with such requirements by market participants.

3.2.2 General macro assessment

FSB Recommendation 16 (implementing OTCD market reforms) recommends that access to trade repository information by official IFIs should be permitted in appropriate form where consistent with their mandates. The IMF, the World Bank and the BIS are official IFIs that foster and support financial stability through general macro assessments of global OTCD markets, sectors or specific countries. Although these analyses may contribute to global financial stability, these efforts may be supported outside an explicit statutory mandate with respect to the oversight, supervision or regulation of a particular market, currency or range of entities. This should not undermine this function or the organisations that perform under it but rather distinguish them from authorities who may access TR data under different functional mandates.

In terms of depth, an official IFI accessing data under this mandate may typically request aggregate-level data across all participants, ie globally, on an anonymised basis. It might be useful to categorise the data by type of counterparty and potentially also country of origin. An official IFI may also have an interest in anonymised position-level data.

3.2.3 Conducting market surveillance and enforcement

The general objective of market surveillance and enforcement is to maintain the integrity of the market by monitoring for, detecting and deterring market abuses such as manipulation or abusive trading that distorts prices or attempts to do so (for example, wash trades or other types of market manipulation), disrupts trading or the physical delivery or cash-settlement of contracts, or otherwise interferes with the transparent, efficient operation of the market. To this end, authorities with a market surveillance and enforcement mandate monitor market activity for anomalous trading activity, including market and price manipulation, insider trading, market rigging, front-running and other deceptive or manipulative conduct. TRs will play a central role in enhancing authorities' ability to effectively monitor market activity for such conduct and in providing the information necessary to support a market authority's enforcement actions.[30]

To carry out this mandate, authorities need to be able to identify and detect unusual or improper trading activities, to analyse trading patterns, and to monitor transactions for abnormal price and volume movements. This type of surveillance generally requires a high degree of granularity. Authorities with a market surveillance mandate would have an interest in various types of information.

They would typically have an interest in transaction-level data consisting in part of cumulative trade event information (including information on the instrument traded, relevant underlier(s), time, price and size of trade, as well as parties to the trade) to identify and detect unusual trading activities, to analyse trading patterns and to monitor for abnormal price and volume movements. For example, detection of wash trades or insider trading will typically require the identification of a series of transactions by a particular entity or entities on a particular underlier or underliers for the suspect time period.[31]

Reference data standards (legal entity identifiers and standard product classifications, for example) would be used to ensure that the trade information is accurate and consistent across market participants and platforms.

In addition, authorities would have an interest in position-level information (in terms of net mark-to-market values) in order to detect large and/or concentrated interest in particular underliers or groups of underliers. Certain forms of surveillance, such as monitoring of position limits, may require information about a given entity's open positions rather than all of its transactions over a specified time period.

An effective surveillance and enforcement programme will also typically require access to transactions involving a fairly broad range of entities and underliers. For example, if an authority is responsible for surveillance and enforcement of illegal trading activities on issuers traded within its jurisdiction, then it will typically have an interest in information on all transactions which have a direct, substantial and foreseeable economic impact on that issuer, regardless of the domicile of that entity or of the counterparties transacting the OTCD. Similarly, an authority will typically have an interest in obtaining access to TR data relating to any transactions that involve counterparties within its legal jurisdiction.

[30] See IOSCO Technical Committee, *Principles for the Regulation and Supervision of Commodity Derivatives Markets – Final Report*, September 2011, p 27, available at http://iosco.org/library/pubdocs/pdf/IOSCOPD358.pdf.

[31] Data Report op cit, p 10. Identification of affiliate transactions may also be required to the extent that a consolidated group engages in OTCD transactions through more than one entity.

Based on these needs, an authority with a market surveillance and/or enforcement mandate will typically have an interest in transaction-level data for transactions involving either underliers within its legal jurisdiction or participants within its legal jurisdiction including their branches and subsidiaries in another jurisdictions.

Identities and names would typically be required. Furthermore, in the event that multiple data productions are required for use in a surveillance and enforcement exercise, these data productions should be consistent in format and easily relatable to one another.[32]

3.2.4 Supervising market participants

The supervision of market participants involves the enforcement of rules and regulations, as well as the monitoring of potentially problematic activities, such as excessive risk-taking.[33] Supervision can be achieved through the regulation and registration of intermediaries, prudential supervision, supervision of market participants with respect to business conduct and compliance with regulatory requirements.

3.2.4.1 Registering and regulating market participants

Some authorities have established or will impose registration (or licensing) standards, capital standards or other financial resources requirements, internal risk management and/or inspection requirements for certain Derivatives Market Intermediaries (DMIs), which may or may not also be prudentially regulated.[34] These requirements facilitate the financial well-being and health of market participants, which in turn enhances the stability of the financial system, by ensuring that authorities have access to relevant information about the structure and operation of key market intermediaries, their financial condition and the risk characteristics of their OTCD activity.

Effective execution of this mandate, including monitoring compliance with these requirements and the reporting obligation, will require access to data that provide an accurate reflection of participants' transaction activity. For example, authorities with a mandate to monitor participants' risk-taking activity will typically require data that allow the authority to quantify and characterise firms' risk-taking activity with respect to particular counterparties.[35] Similarly, authorities with a mandate to ensure compliance with a registration requirement will typically require data regarding transactions of non-registered participants that are engaged in OTCD activity within the market over which it has legal jurisdiction. For example, monitoring compliance with a registration requirement will require the authority to have access to data involving any potential registrants. Monitoring compliance with capital or inspection requirements and risk-taking generally apply only to registered participants and thus, in many cases, will require access to data regarding transactions to which a registered participant is a counterparty. Similarly, authorities will typically need access to transaction-level data regarding entities within its legal jurisdiction to ensure such entities are complying with OTCD transaction-reporting requirements.

Given the potential for a market participant to evade these supervisory requirements by trading with related entities, authorities exercising this mandate will also typically require access to data

[32] For example, an analysis of the order book of an organised trading platform may incorporate the completed trade record, the cancelled trade record and the order book itself, which are sometimes maintained as separate documents with differing field name conventions and data formats.

[33] More than one authority in one or more jurisdictions may have a mandate to regulate or supervise a given participant. Each authority would typically have an interest arising from its respective mandate in accessing data related to that participant as detailed in the discussion below, and this interest should not be prejudiced by another authority's possession of a similar or overlapping mandate with respect to the same participant.

[34] Some of these requirements are described in the IOSCO Report on DMIs, which sets out 15 recommendations for effective regulation of these participants.

[35] CPSS-IOSCO Data Report op cit, p 11.

involving the transactions of entities with which the participant enters into OTCD transactions or whose OTCD transactions it guarantees.

Based on these needs, therefore, an authority with a mandate to regulate market participants will typically have an interest in transaction-level data for transactions involving participants within its legal jurisdiction. To the extent that a participant enters into OTCD transactions with related entities or guarantees the OTCD transactions of such entities, authorities may also have an interest in data relating to transactions to which such entities are a counterparty. Identities and names would typically be required.

In implementing regulatory requirements for market participants, authorities will require TR information for eligibility determination, monitoring, surveillance and inspection. TR data regarding positions or trading patterns of a non-registrant, for example, can provide a regulator with information that may help, to the extent it is relevant, in determining a registration obligation.

3.2.4.2 Supervising market participants with respect to business conduct and compliance with regulatory requirements

Some authorities have established, or will impose, business conduct and other regulatory requirements on market participants. These requirements may include a duty to implement policies and procedures designed to control and manage risk; to assess counterparty or client suitability; to disclose inducements; to act with the requisite degree of expertise, care and diligence in dealings with counterparties or clients; to ensure all marketing and communications to counterparties or clients are fair, clear and not misleading; and to safeguard the interests of, and provide adequate information to, counterparties or clients.[36] IOSCO has recommended that DMIs be subject to various business conduct, business supervision, and record-keeping standards.[37]

Based on these needs, effective execution of this mandate, including monitoring compliance with these requirements, will require an authority with a mandate to supervise or regulate the OTCD business conduct of market participants to typically access transaction-level data for market participants within its legal jurisdiction.

3.2.4.3 Prudentially supervising financial institutions

A prudential supervisor[38] is responsible for supervising and regulating or monitoring and conducting surveillance on financial institutions to ensure they are in sound financial condition, to promote the adoption of policies and procedures designed to control and manage risk, and to monitor and evaluate system-wide or sectoral issues that may impact these institutions negatively. Many market participants are subsidiaries of consolidated, multinational organisations.[39] Jurisdictions provide for the prudential supervision of the consolidated organisation, which in turn requires the need for risk information pertaining to the parent entity and each subsidiary entity within the consolidated organisation.

[36] IOSCO, *International Standards for Derivatives Market Intermediary Regulation*, p 23.

[37] Op cit, Recommendations 8–15.

[38] In addition, where authorities have the capacity to obtain transaction-level data directly from financial institutions based on their mandates, TRs should ensure the access by such authorities to transaction-level data of the relevant financial institutions.

[39] The term "subsidiary" will here denote an affiliate for which the holding company maintains a controlling interest in that affiliate. An affiliate should be differentiated from a branch. In the scope of this report, the term "affiliate" will denote a legal entity that is incorporated or otherwise organised under the company or business association law of a territorial jurisdiction; the term "branch" will denote an office of a legal entity that is considered physically remote from the main office of that legal entity, but which is not a separate legal entity. Authorities and TR operators should take special care to note that some legal entities (ie affiliates) sometimes contain the word "branch" in their legal name.

If an authority is responsible for the prudential supervision of a consolidated organisation whose parent entity is in its legal jurisdiction, then that authority will typically require, for each subsidiary entity in the entire organisation, access to TR data that is equivalent to the access it has to TR data for the parent entity, regardless of the country of domicile or primary supervisor of that subsidiary entity, at the transaction level.

If an authority is responsible for supervision of a subsidiary entity of a foreign prudentially supervised consolidated organisation, then that authority will typically require access to TR data regarding the local subsidiary at the transaction level. Identities and names would typically be required.

3.2.5 Regulating, supervising or overseeing trading venues and financial market infrastructure

The establishment of trading systems, including exchanges, organised markets and organised trading platforms, is subject to regulatory authorisation and supervision. There is also ongoing regulatory supervision of exchanges, organised markets and organised trading platforms that aims to ensure that the integrity of trading is maintained through fair and equitable rules that strike an appropriate balance between the demands of different market participants.[40]

FMIs play a critical role in the financial system and the broader economy. While safe and efficient FMIs contribute to maintaining and promoting financial stability and economic growth, FMIs also concentrate risk. If not properly managed, FMIs can be sources of financial shocks, such as liquidity dislocations and credit losses, or a major channel through which these shocks are transmitted across domestic and international financial markets.[41]

3.2.5.1 Exchanges, organised markets and organised trading platforms

OTCD transactions may be conducted on regulated trading platforms. Authorities which regulate, supervise or oversee such trading platforms may require access to data pertaining to transactions conducted on these facilities.

If an authority regulates, supervises or oversees an exchange, an organised market or an organised trading platform, then that authority would typically have an interest in data for transactions conducted on that exchange, organised market or organised trading platform based at the transaction level.[42] For example, to address market integrity concerns, authorities may need to reconstruct trades and create an audit trail. In order to do so, it would be necessary to have full transaction-level details. Named data would be necessary to map the participants to the trading platform and the counterparties to the transactions registered in the TR.

3.2.5.2 Payment or settlement systems

Payment and settlement systems enable the transfer of money and financial instruments. Safe and efficient systems are fundamental to money being an effective means of payment and to the smooth functioning of financial markets. Well designed and managed systems help to maintain financial stability by preventing or containing financial crises and help to reduce the cost and uncertainty of settlement, which could otherwise act as an impediment to economic activity. Payment and settlement systems thus play a crucial role in a market economy and some authorities have always had a close interest in them as part of their responsibilities for monetary and financial stability. Oversight of payment or settlement

[40] See IOSCO, *Objectives and Principles of securities regulation*, 2010, http://www.iosco.org/library/pubdocs/pdf/IOSCOPD154.pdf.

[41] See CPSS-IOSCO PFMIs, p 5.

[42] The supervisor of the exchange, organised market or organised trading platform may also have market surveillance and enforcement mandates.

systems would typically require data that allow them to understand, assess and monitor the activities of payment or settlement systems and their participants, including the risks created and borne by the system and, where appropriate, its participants, and the system's impact on its participants and the broader economy.

Payment flows associated with OTCD transactions settle over payment systems. In normal times and during market events, the overseers of these systems would typically need data to understand the volume of activity that will flow over the system including potential peaks or other stresses that may introduce risk to the payment system or other linked systems.[43]

Authorities would typically need access to all TR data involving payment obligations in currencies in which payments are conducted over the systems for which the authority has responsibility.[44] In terms of depth, authorities would typically require position-level data. Position-level data could remain anonymised in the initial data requests, but the authority should have the ability to access named data if needed, for example, on counterparties of the central bank where named data would be required and where the analysis of position-level data leads the authority to investigate suspicious activity. In order to be able to monitor payment flows, authorities may also have an interest in anonymised transaction-level data for participants in payment and settlement systems.

3.2.5.3 CCPs

Authorities that regulate, supervise or oversee CCPs would typically have an interest in data pertaining to transactions cleared by these facilities.

Given the critical function that CCPs play in the OTCD markets, authorities that regulate, supervise or oversee these entities need to ensure the safety and efficiency of the CCP itself or its compliance with relevant regulatory requirements. Most of the risk management functions handled by a CCP, such as exposure calculations and margining, are based on the transactions cleared by the entity. Although authorities will need more than data held in a TR to effectively look at a CCP's management functions, an authority will require full access to the TR data on underlying transactions, to enable it to confirm the risk borne by the CCP and evaluate the risk management functions of the CCP.

In terms of depth, these authorities would typically need transaction-level access to all TR data where the CCP is identified as the counterparty or, if the CCP is not identified as the counterparty to the two original parties, where such trades are identified as being cleared in that facility. In terms of breadth, an authority will require access to all transactions cleared through the CCP on a global level. Named data would be necessary to establish the connection between the counterparties (and any intermediaries such as executing or prime brokers) and the OTCD transactions cleared by the CCP.

3.2.5.4 TRs

The functions involved in regulating, supervising or overseeing a TR typically involve supervision of the TR platform itself (eg operational risk management) and require the TR supervisor to be able to access any data in the TR, including any data reported to the TR. In carrying out these responsibilities the supervisor's access to TR market data would be designed to assist the supervisor in assessing the TR's compliance with applicable requirements.

[43] In some circumstances, authorities that regulate, supervise or oversee central securities depositories or securities settlement systems may require access to TR data with regard to OTCD transactions that are physically settled and result in securities movements.

[44] Access by authorities to the data elements related to payment obligations (eg settlement currency under master agreement netting provisions, or credit event settlements resulting from bankruptcy or restructuring) is subject to the data being actually reported to TRs.

An authority with a TR supervision mandate will typically have an interest in all transaction-level data reported to the TR that it supervises. Named data will typically be required where the TR supervisor is performing testing for supervisory purposes. For example, a TR supervisor may want to verify that the TR is following international standards for unique identifiers, such as LEIs.

3.2.6 Planning and conducting resolution activities

Regulated entities that are counterparties to OTCD transactions may be subject to specific resolution processes in the event that an entity is no longer viable and has no reasonable prospect of recovery. To minimise the potential impact of a firm's resolution on the financial system, the disposition of OTCD transactions in the resolved entity's portfolio may be subject to statutory or regulatory time limits, requiring a rapid determination of treatment by the authority administering the resolution. Accordingly, the resolution authority must be able to obtain access and monitor appropriate TR data, generally as part of pre-resolution planning activities and during the conduct of resolution activities for an insolvent entity.

Carrying out the resolution of an entity involves ascertaining the obligations of that entity to different counterparties and settling the claims of those counterparties using a transparent and non-discriminatory set of rules. To that end, authorities need to identify all the trades of the defaulting entity, identify all the counterparties to the above-mentioned trades, and determine counterparty exposure. Having access to TR data will assist the resolution authority in determining all outstanding positions for OTCD transactions.[45]

An authority with a resolution mandate will typically have an interest in named transaction-level data for all transactions within the scope of the resolution proceedings.

3.2.7 Implementing monetary policy and lender of last resort function

3.2.7.1 Managing currency policy

Some authorities typically need access to data based on currency of settlement to fulfil currency policy management. Among other things, an authority responsible for a currency is interested in information related to monitoring aggregate or individual payment flows affecting payments and settlement systems; monitoring the liquidity of that currency, and monitoring for speculative activity in that currency. This will be especially useful to assess the potential liquidity strains that may have an impact on the implementation of monetary policy.

The central bank of issue for a currency will typically be interested in data for transactions that specify settlement in that currency, including transactions for which that currency is one of two or more specified settlement currencies, at an anonymised position-level in that currency. Anonymised transaction-level data may also be requested, particularly when the aim is to detect speculative activity in the related currency.

3.2.7.2 Implementing monetary policy

Central banks typically conduct monetary policy to achieve broad macroeconomic objectives. Monetary policy objectives are typically specified in statute and generally direct the central bank to focus on goals such as price stability, sustainable economic growth and full employment. In normal times, most central banks conduct policy by managing the level of short-term interest rates through appropriate open market operations. Central banks rely on a broad range of data to inform their monetary policy decisions including a wide array of data on financial markets and statistics on the prices of goods, services,

[45] As set out in the FSB's *Third Progress Report on Implementation on OTC Derivative Markets Reform*, one of the four broad categories that were identified by the ODEG is information on the assets used to collateralise OTCD transactions.

materials and labour in a particular country or currency zone. A central bank may be interested in OTCD data to broadly understand the activity and risks in financial markets and this information could be useful in the conduct of monetary policy. In this regard, a central bank may request access to aggregate-level data on underliers denominated in its currency and participants within the central bank's legal jurisdiction or geographic location of participants on an anonymous basis.

3.2.7.3 Acting as lender of last resort

Central banks are the ultimate providers of liquidity in their respective currencies. In deciding whether to lend to a particular institution, a central bank would consider a number of questions including the nature of the liquidity need, the types of collateral available to pledge to secure the loan, solvency of the borrower and any legal constraints. In an emergency situation, the central bank may also need to consider whether the loan is necessary to address potential systemic consequences. Position-level information involving the potential borrower could inform policymakers' views on these questions. In the OTCD context, this could include data on the named institution as counterparty to OTCD transactions as well as aggregate data and the depth of liquidity in the market in order to understand the potential repercussions on a particular market and potential knock-on effects if liquidity is denied.

3.2.8 Conducting research supporting the above functions

Many authorities conduct research on the markets that they have responsibility for under the mandates listed above and will typically conduct research using TR data under these functional mandates.

In order to perform research that can effectively support their mandate(s), authorities may from time to time need to issue non-typical data requests for research purposes that go beyond the typical requests in relation to the underlying mandate for which they are requesting data. In such cases, such data requests would generally be focused on time-lagged data, ie on historical transaction/position/aggregate-level data.

Any publication of the research or outcome of the research and analysis that uses TR data will need to respect the confidentiality of data with the utmost care. In particular, the product that results from this research should safeguard against invertibility, that is, recipients of the work product should not be able to recalculate the original transaction-level data and any published research should be fully anonymised and aggregated. TR data accessed for research purposes should not be shared beyond the research function.

4 Approaches to facilitating authorities' access to TR data

This section addresses three issues that may create obstacles to practical and effective access to TR data and cause some authorities to be reluctant to allow participants under their authority to report certain transactions to TRs outside their jurisdiction: procedural constraints of accessing TR data, legal constraints to such access and the confidentiality concerns related to data reported to the TR. This section also discusses some options and safeguards to address these issues, including the particular roles that TRs, TR supervisors, and requesting authorities may play in this respect.

4.1 Addressing procedural constraints to OTCD data access

Procedural constraints may result from a lack of clear policy or procedures for obtaining access to TR data. For example, these constraints may include lack of clarity as to how a requesting authority could demonstrate its mandate to the TR holding the OTCD data or its supervising authority, or a delay in obtaining access to data due to operational or other issues.

4.1.1 Role of the TR

Different jurisdictions may have different approaches regarding the role and degree of involvement of a TR in determining the level of access of an authority to data. In some jurisdictions, the legal framework may define the scope of entities that can obtain access to data in a TR located in that jurisdiction. The relevant authorities may have rules on how such access may be achieved and the TR would be expected to implement its procedures in a manner that is consistent with the local regulatory requirements and which allows the TR supervisor to check that the procedures are in compliance with its rules. In other jurisdictions, the legal framework may be less prescriptive, with the expectation that the TR will develop policies and procedures in a manner that is in line with the PFMI and the guidance outlined in this report.

In general, this report is intended to guide TRs in providing data to authorities in a manner compatible with the TR's legal framework, and it assumes that the legal framework supports access in high-level terms, and that the TR will establish a robust process appropriately governed to support its role in facilitating the provision of data to authorities. By setting out a common understanding on typical data requests arising from various functional mandates, this report aims to achieve consistent outcomes concerning authorities' access to data regardless of the regulatory/legal framework of the jurisdiction in which the TR is located. Thus, the guidance and data access mapping in this report should be applied consistently where access is determined (i) in the legal framework or regulatory rules, (ii) by TR supervisors, or (iii) by TRs.

In operational terms, TRs should implement effective processes and procedures related to facilitating effective and practical access to the data they maintain while protecting confidential information, under conditions specified under Principle 24 of the PFMI.

4.1.2 Role of the TR supervisor

A TR supervisor should strive to ensure that the TR's processes and procedures for access to data take into consideration any applicable standards and internationally accepted principles including the guidance and data access mapping set out in this report.

As a general matter, TR supervisors should avoid acting as gatekeepers to data held in a TR if this is not required by law and they should avoid actions that could hamper another authority's timely access. Where a TR supervisor is required by law to be involved in determining the scope of access by other authorities, it should strive to ensure that access is provided to the requesting authority in a manner consistent with the guidance in this report to the maximum extent permitted by law. Once such determination has been granted to a requesting authority, the TR supervisor is not expected to be involved in validating typical individual requests from those authorities.

4.1.3 Role of the requesting authority

Requesting authorities should be able to clearly articulate their mandate(s) to a TR, such that the information needs associated with the access might be reasonably understood to facilitate a rational, consistent and appropriate response from the TR. A requesting authority should also be prepared to provide the TR with the standard information it seeks as part of the TR's process to respond to an authority's data request. As noted above, such requests should be designed to allow the TR to confirm the nature of the authority's mandate(s). However, the TR should not have discretion over the level of access that each requesting authority is granted.

Requesting authorities with multiple mandates should consider the need to maintain separate operational access requests to TR data for each of their functional responsibilities. To facilitate appropriate access to data within an authority, an authority with multiple mandates that is likely to make multiple types of data requests in support of these various mandates should consider developing internal procedures or identifying a central coordinating area for TR data requests. Such a central

coordinating area could help to ensure that the appropriate internal access levels are set up with the TR to support the authority's various functions.

As part of their mandates, authorities may make data requests that fall within the "typical" access levels for a given mandate (as set forth in the data mapping table), while other requests may not be described as "typical" within this report. Typical data requests are considered those that TRs are likely to receive by authorities to support their needs for a given mandate. Non-typical data requests may be motivated by a particular set of circumstances that require an unanticipated type or range of data, or are otherwise outside of the scope of data requests authorities are typically expected to make with respect to a particular mandate. It is also important to acknowledge that requests that may be viewed as "non-typical" today may become "typical" in the future.

4.2 Addressing legal constraints

An authority requesting access to TR data may face various legal obstacles to its access to OTCD data held in a TR. Of these obstacles, three are of particular significance. First, domestic laws and regulations may not always provide for the full provision of information, in accordance with this report, directly from TRs to authorities. This may be due to the effect of blocking, secrecy, privacy statutes or confidentiality requirements within a particular jurisdiction. Second, the TR may be required by law or regulation to obtain indemnification from third-country or domestic authorities before sharing data, which such authorities may not be authorised or willing to provide. Third, even without an explicit indemnification agreement, a requesting authority or its staff may be required to comply with certain confidentiality constraints, imposed by either contract or law, that may also expose them to legal liability, including possibly criminal liability, in the case of a requesting authority's own breach of confidentiality undertakings or laws. These legal obstacles and liability concerns are all the more complex when the requesting authority is not located in the same jurisdiction as the TR.

These legal obstacles may preclude TRs in such jurisdictions from providing critical market data to certain authorities. Efforts should be made to remove any legal obstacles or restrictions to enable effective and practical access to data by relevant requesting authorities, provided such authorities are subject to appropriate confidentiality safeguards. In case of remaining legal obstacles, the use of the following safeguards may be contemplated.

4.2.1 Mitigating liability and other legal obstacles

Certain potential legal obstacles, including the requirement to obtain indemnification and for blocking, secrecy, privacy or similar requirements, that may prevent authorities from accessing data in a TR (whether on a cross-border or domestic basis) may be mitigated in a number of ways. It may be possible to adapt the legal framework to remove or mitigate such requirements, for authorities accessing data under their respective mandate(s). Another option may include allowing a TR not to impose blocking, secrecy, privacy or similar requirements, or not to require indemnification under specified conditions, where consistent with national law, to ensure relevant authorities can have direct and continuous access to the data under their mandate.[46]

4.2.2 Alternative methods of ensuring access to relevant data

In instances where direct access by an authority is blocked because of legal constraints on direct access, the legal framework may provide for indirect access via another authority, which will typically be a TR supervisor or another authority having direct access to the data. In such circumstances, indirect access

[46] The Joint Communiqué of the 18–19 April 2013 G20 meeting of Finance Ministers advocates that legal obstacles to access are addressed: *"Jurisdictions should remove barriers to trade reporting by market participants, with particular attention [to removing barriers to reporting of counterparty information and] to information access by authorities."*

may be a second best solution to address these situations, but it should be viewed as the exception, not the norm. If legally permitted, TR supervisors may be able to play a role in assisting requesting authorities to obtain appropriate indirect access to data in support of their mandates.

One consequence of restrictions on access to named position and transaction-level data outside the authority's jurisdiction is that authorities may not have a complete view of transactions or positions of entities that may have a direct effect on the OTCD market within their jurisdiction; as a consequence, transparency to authorities may be limited to that part of the network that is within a particular jurisdiction, which may not be sufficient to ensure adequate regulation, supervision or oversight of entities within each authority's legal jurisdiction. A fallback solution regarding the limitation of access to anonymised data outside the authority's jurisdiction would consist in seeking agreements with other jurisdictions to reciprocal data sharing outside TRs.

In case an indirect access channel has to be used, the information that the requesting authorities would typically require should be provided on a timely basis, as provided for in this report. It is recognised that authorities providing information to requesting authorities may need to ascertain that the requesting authorities will take appropriate steps to ensure the confidentiality of this information.

Authorities with access to TR data should accordingly take steps to ensure they have appropriate arrangements in place with other authorities with whom they are likely to need to share TR data, consistent with the framework for cooperation set forth in Responsibility E of the CPSS-IOSCO PFMI. By ensuring these arrangements are in place, authorities should be better able to ensure that they can share relevant TR data with authorities on a timely basis. Where practical (and allowable under relevant laws), authorities should also consider the provision of relevant TR data to other authorities on an ongoing basis to allow authorities to meet their mandates.

4.3 Addressing confidentiality concerns

4.3.1 Confidentiality concerns related to TR data access

The commitment to the development of OTCD data reporting is intended to improve the effectiveness and the practicality of the way authorities perform their mandates. However, the reporting of data to TRs also raises confidentiality concerns associated with the reported information. As noted above, sensitive information provided by reporting entities directly to authorities has typically been accorded confidentiality protections by statute or regulation that limits the use and dissemination of this information. As an expanded set of authorities rely on TRs for data, it is of particular concern that the data are treated confidentially and used appropriately by authorities according to their respective mandates. As TRs will very likely store cross-jurisdictional information that may be accessed by an expanding set of authorities, it is critical to ensure the necessary confidential treatment of the data reported to TRs. In addition, some authorities may typically combine different mandates. Where an authority has more than one mandate, the process to validate under which specific mandate a data request is made could be complex, in practical terms.

As such, it is important to identify any associated issues that could raise concerns and appropriately address them to allow for authorities' effective access to TR data. Because of legal and regulatory confidentiality requirements, each requesting authority's access should be within the applicable law and regulation and consistent with its mandate(s).

The potential access to information by authorities may depend on the proximity with respect to the constituents of TR data (counterparty, underlier). As this proximity diminishes or becomes less obvious, confidentiality concerns may increase. This applies especially to entity-specific information,

which would be otherwise highly confidential and typically accessible only by the supervisors of the reporting entity.[47]

However, given the global scope of OTCD markets, their relevance for global financial stability, and their significant implications for major financial institutions and market infrastructures, the data stored in TRs will likely support a range of other public policy objectives across different jurisdictions. To fulfil their tasks, some authorities (eg those responsible for a currency, for monetary policy, for the oversight of payment or settlement systems, for systemic risk analysis and macro prudential regulation, and oversight/supervision of CCPs) would require, in order to fulfil their tasks, access to a certain breadth and depth of data across participants and underliers, which would not lend itself to a narrow jurisdictional view.

Additionally, since TRs constitute important FMIs, they will be supervised by authorities that have direct statutory authority for supervising and regulating a TR. Because the responsibilities of a TR supervisor relate to the TR itself, in the course of performing this task this TR supervisor would typically have full access to all data of participants in the different jurisdictions that allow reporting of OTCD transactions in that TR, at the most granular level. The TR supervisor would have access to information that it would not have access to otherwise, as a requesting authority accessing data directly from the reporting entities.

4.3.2 Confidentiality safeguards

As a general principle, authorities' accessing TR data should assure that the requested data are subject to appropriate regulatory regimes protecting the confidentiality of the information.

4.3.2.1 Mitigating confidentiality concerns

An authority that receives data which identifies reporting entities should strive to ensure that it applies the appropriate protections to the use of the data and that it is treating the data in a manner consistent with its confidentiality policies.

Authorities are generally subject to statutory obligations regarding the use of confidential information. These obligations generally require authorities receiving confidential information to use it only in the performance of their duties and for the exercise of their functions. Authorities could address confidentiality concerns relating to access to TR data by ensuring that transmissions of confidential TR data within the authority conform to the authority's policies governing use of confidential information and that all relevant functions are subject to the same confidentiality provisions. Clarity with regard to such provisions could also alleviate confidentiality concerns with respect to TR supervisors.

Where an authority has multiple mandates, access to data necessary to fulfil those mandates should be consistent with that authority's internal procedures for information-sharing across functional areas. This aims to ensure adequate information flows, encourage collaborative analysis, discussion and policy development, and to ensure consistent implementation of policy instruments and effective enforcement.[48] Confidentiality concerns could arise if the different functions of an authority that

[47] For example, the data submitted by a reporting entity to a TR might be equivalent to data that supervisors of the reporting entity and authorities with the responsibility of market surveillance of affected financial instruments/underliers would collect and handle pursuant to strict confidentiality requirements if such data were reported directly to those supervisors or authorities. Based on this equivalence, data requests of such authorities related to data of their supervised entities and within their legal jurisdiction should not therefore lead to confidentiality concerns.

[48] Information-sharing practices within authorities range from no restrictions on sharing data (other than the compulsory condition of the purpose for performing the respective duties) to strict firewalls. Usually, there would be internal processes and procedures to ensure that staff obtains access only to data that they are authorised to view (based on the data needed by them to fulfil their duties). However, even authorised institutions-specific information or transaction-level information on individual financial institutions, which would be usually restricted to authorised staff, could often be shared with other functions if necessary for fulfilling the mandate or in a particular situation.

articulate a need for TR data of differing scope and granularity do not have in place appropriate safeguards for confidential data.

Authorities should mitigate confidentiality concerns with respect to any confidential information received, exchanged or transmitted by authorities by taking steps to ensure that no confidential information received in the course of their duties should be divulged to any person or authority, except in summary or aggregate form such that an individual reporting entities cannot be identified, except to the extent permitted or required by law.

4.3.2.2 Addressing the specific confidentiality requirements of central bank operations

Central banks perform a wide variety of financial transactions in order to fulfil their functions. The main core policy functions include monetary policy implementation, lender of last resort/emergency liquidity assistance, FX intervention and reserve management (for some central banks), and possibly others depending on the specific mandate of the central bank. Some central banks may also carry out non-core transactions (eg certain investment transactions) that are less sensitive from a policy perspective.

OTCD transactions could potentially be used in relation to many, if not all, of the transaction types listed above, and could thus potentially be reported to a trade repository (either by a central bank's counterparty, or by both the central bank and its counterparty).

While certain jurisdictions exempt central banks from OTCD data-reporting requirements, such exemptions may not apply to their counterparties. Other jurisdictions may include foreign central banks in the scope of the reporting requirement. Therefore, in many jurisdictions, transactions with central banks would be included, directly or indirectly (through the reporting of central banks' counterparties) in the data set stored at TRs.

To fulfil their policy mandates effectively, central banks would typically want to retain control over the terms (timing, pricing, counterparty, collateral, haircut etc) on which they perform their core transactions. Since these transactions often have significant policy and/or market news content, it is crucial for central banks to be able to control whether, when and how information about their actions are disclosed so as to maximise the intended impact and limit any unintended impact. In the context of TRs, any access by authorities to data involving central bank transactions must not compromise confidentiality where confidentiality is due.

It is acknowledged that some authorities may already have access to partial information on central bank transactions under decentralised or market reporting when obtaining information from central bank counterparties, and the guidance set by the report does not aim to limit such access.

Therefore, an approach that will increase the confidentiality of central bank transactions, minimising at the same time the impact on the information availability for the different authorities consists in introducing: (i) limitations on authorities' access to central bank information and (ii) an enhanced confidentiality regime for information on central bank transactions obtained from a TR.

Limitations on authorities' access to central bank information: authorities should avoid submitting or making data requests with transaction- or position-level data focusing on a central bank as the entry point of the transactions. This limitation will ensure that a comprehensive view of the operations of a particular central bank remains confidential. It will also ensure that authorities retain access to transaction-level data on those central bank transactions that are already accessible to them through the decentralised reporting of the counterparties of the relevant central bank.[49] Authorities will

[49] Under a decentralised reporting framework, an authority may obtain information on central bank transactions from the reporting of the central bank's counterparties. It is understood that these operations will be available to the respective authority, and will be included in the reports focusing on the activity of the entity, which will include the trades of this entity with any counterparty, potentially including central banks.

also make a high priority of not taking actions that would undermine central bank operations carried out in pursuit of their mandates concerning monetary policy and financial stability.

Enhanced confidentiality regime for information on central bank transactions obtained from a TR: authorities receiving transaction- or position-level data concerning central bank transactions from a TR should have in place reasonable measures to ensure that this information (i) is available only to those functional areas that need that information for the performance of the mandate under which this information was obtained (if an authority has several mandates, information concerning central bank transactions should not be exchanged internally between the units in charge of different functions, except to the extent that each unit could independently obtain such data under its mandate), and (ii) is not made public or transmitted to third parties, except to the extent unavoidable under law (public reports based on this data should not contain information that could lead to the identification of any central bank).

4.3.2.3 Role of the TR supervisor in addressing confidentiality concerns

Authorities with explicit legal or statutory responsibility over a TR would likely have authority to obtain access to any information in the TR that is necessary to carry out supervisory and regulatory responsibilities vis-à-vis the TR. In some instances, the supervisory regime applied may involve access to the full books and records of the TR, and such access would include all of the data held by the TR. There is no presumption that such authorities should seek to limit or constrain their statutory authorities or responsibilities, and in many jurisdictions, such limitations would not even be permitted under applicable law.[50]

To address confidentiality concerns, however, a TR supervisory authority may consider one or more of the following practical processes for handling data it has access to as a TR supervisor, where allowable by law. For example, a TR supervisory authority that has multiple functions may in practice consider the need to maintain separate operational access requests to TR data for each of its functional responsibilities. Another practical option relates to the TR supervisory authority's use of data. A TR supervisory authority may need to be able to access all data held by a TR under its supervision in order to fulfil its statutory mandate, and check that the data being reported is compliant with its jurisdiction's supervisory requirements. However, authorities may consider whether it is necessary to retain data accessed under this mandate beyond the period needed to perform such checks. Therefore such authorities may consider performing testing of data ("transaction testing") as a general practice, and not retaining the reviewed data samples strictly beyond the testing procedure, where consistent with applicable law, without precluding the need to allow for a longer retention period in cases where tested material may call for further action.

Such understanding among authorities and practice by supervisors of TRs are intended to address potential concerns regarding a TR supervisor's full access to data that originated from another jurisdiction.

To the extent that access to TR data is extended to organisations responsible for performing a mandate pursuant to a statutory delegation of authority, as described in Section 3 of this report, the legal framework should ensure that the organisation can comply with confidentiality rules. Additionally, the organisation's supervising authority may consider whether it would be appropriate to identify which of the organisation's directors, officers, employees, sub-contractors and professional advisers need to have access to the information from the TR in the proper exercise of their respective roles and duties.

[50] Moreover, if a TR supervisor becomes aware of an issue based on information data obtained in the normal course of TR supervision, the TR supervisor's policies may require referral of that information either internally or to the relevant authority with responsibility for the counterparties or underliers to the transaction.

5 Framework and guidelines for authorities' access to TR data

The guidance in this section has been developed within the existing international framework for OTCD. Specifically as noted previously in this report, FSB recommendation 16 states that, "market regulators, central banks, prudential supervisors, and resolution authorities must have effective and practical access to the data collected by trade repositories that they require to carry out their respective regulatory mandates. Access to trade repository information by official international financial institutions also should be permitted in appropriate form where consistent with their mandates."[51]

5.1 Existing international framework and standards

Consistent with the G20 commitments and FSB recommendations with regard to OTC derivatives, CPSS-IOSCO developed international standards for FMIs, which include principles applicable to TRs and responsibilities for relevant authorities. The expectations set forth support the objective of facilitating effective and practical access to TR data by authorities.

FSB, Recommendation 16

Market regulators, central banks, prudential supervisors and resolution authorities must have effective and practical access to the data collected by trade repositories that they require to carry out their respective regulatory mandates. Access to trade repository information by official international financial institutions also should be permitted in appropriate form where consistent with their mandates.

PFMI Principle 24, Key Consideration 2

A TR should have effective processes and procedures to provide data to relevant authorities in a timely and appropriate manner to enable them to meet their respective regulatory mandates and legal responsibilities.

The provision of data from a TR to relevant requesting authorities should be supported from a legal, procedural, policy, operational, regulatory and technological perspective. A TR should have objectives, policies and procedures that support the effective and appropriate disclosure of market data to relevant authorities. To promote data access that is effective and practical across the range of requesting authorities, TRs should establish, maintain and implement clearly articulated and rationalised access policies. These policies should be transparent to all TR stakeholders, including participants reporting data to a TR and authorities requesting data from a TR.

In its policies and procedures, TRs should clearly articulate and disclose to all relevant authorities and stakeholders the standard set of information that requesting authorities should provide to the TR in conjunction with the requesting authority's request for data. Such information may include an articulation of the requesting authority's mandate, the specific relevant data it seeks, and confirmation that the authority will be able to protect the confidentiality of information it receives. A defined set of standard information provided by all requesting authorities would facilitate transparency and consistency in responding to data requests from authorities. It also would provide TRs with information on which it would base its validation and authorisation in response to data requests. TRs

[51] FSB *Implementing OTC derivatives market reforms* 25 October 2010.

should also make available, to the community of authorities that use them, the list of authorities that either register or recognise the TRs.

TRs should support arrangements that promote appropriate access that are consistent with approved policies and procedures. The TR's governance process should be clear as to who is accountable for monitoring compliance with and enforcing the TR's data access policy. Decisions regarding the level of access to data by a particular authority or type of authority for requests that are not defined as typical may depend on the regulatory regime of the TR. In the circumstances where there is significant uncertainty or the TR's established governance process is unable to resolve a question on how to address a non-typical data request from an authority, some jurisdictions may give a role to the TR's supervisor to provide specific guidance.

A TR should put in place a process to consider and appropriately respond to requests for data that fall outside the scope of the guidance provided by the data mapping in section 6. Such a process should include escalation steps within the TR and may involve the supervisor of the TR, as appropriate.

A TR's access policy may need to reflect certain legal or other restrictions, however it should make an effort to enable appropriate, effective and practical access to data by relevant authorities to the maximum extent permitted by law, provided such authorities are subject to appropriate confidentiality safeguards.

PFMI Responsibility E, Key Consideration 8

Relevant authorities should coordinate to ensure timely access to trade data recorded in a TR.

A TR supervisor should ensure that the TR's processes and procedures for access to data are consistent with any applicable standards and internationally accepted principles including the supporting recommendations and guidelines, and data access mapping set out in this report. In general, it is not expected that a TR supervisor would seek to limit access levels beyond what is contemplated in this report, but such authority may seek to ensure that any policies and procedures of the TR are consistent with the applicable legal framework with due regard to confidentiality safeguards and mandates of requesting authorities. Specifically, the supervisor of a TR that maintains data pertaining to other jurisdictions should coordinate with other relevant authorities to ensure timely and effective access to trade data and establish an appropriate data access process that is fair and consistent with the responsibilities of the other relevant authorities, to the extent legally permissible. Consistent with the CPSS/IOSCO Responsibility E, all relevant authorities should mutually support each other's access to trade data in which they have a material interest in furtherance of their regulatory, supervisory and oversight responsibilities, regardless of the particular organisational form or jurisdiction of a TR.

Where a TR supervisor is required by law to be involved in determining the scope of access by other authorities, it should ensure that access is provided to the requesting authority in a manner that is consistent with the guidance in this report. In some jurisdictions, the legal framework in which the TR operates may dictate the level of access that different authorities may have to data in the TR. In instances where the legal framework does not provide for direct access to certain types of authorities, a TR supervisor may be able to play a role in assisting these authorities to facilitate appropriate access to data in support of their respective mandates. When this situation arises, authorities with full access to TR data (generally a TR supervisor) should ensure that requesting authorities have access to the information relevant for the requesting authority as provided for in this report.

5.2 Access guidelines

Access levels consistent with authorities' mandates:

Authorities that require information on OTC derivatives transactions in order to carry out their respective mandates should have sufficient and timely access to relevant data.

Where authorities are involved in the process of developing the legal framework and local rules for determining access levels, they should aim to ensure that such rules ensure sufficient and timely access to relevant data by requesting authorities, consistent with their respective mandates.

Given that several authorities perform multiple mandates, the nature of an entity itself, whether a market authority, prudential authority, central bank, or other, may not in itself be sufficient to articulate access levels. Each authority's minimum access privileges under each of its mandate should not be prejudiced by the fact that the authority is responsible for multiple mandates requiring access to TR data. Similarly, an authority's minimum access privileges under a given mandate should not be prejudiced by the fact that one or more other authorities may also be responsible for performing that mandate.

To the extent that a TR holds data regarding participants located in other jurisdictions, as a matter of principle a TR supervisor will not purposefully and deliberately access data for a purpose that is not related to the authority's supervisory responsibilities.

TRs should remain flexible in responding to changes in the mandates and responsibilities of authorities that access, or may in future seek access to, TR-held data. Because the market is changing, some new concerns and interests may also emerge and evolve from time to time, warranting a different access level even without any change in the authority's mandate. These legitimate factors should be distinguished from a data request that falls outside or beyond the authority's mandate.

Confidentiality safeguard:

Authorities obtaining access to data should have the ability to keep the data confidential.

The centralised storage of OTCD data underscores the importance of confidentiality constraints associated with handling of market participant data. Confidentiality protections typically limit the use and dissemination of sensitive information provided by reporting entities directly to authorities. In order to ensure the same level of confidentiality protection for the data reported by a TR, authorities accessing data in the TR should have the legal right and the ability to keep the data confidential, and it should take all reasonable steps to do so. This would not prohibit authorities from disclosing data if required or permitted to do so by law.

Non-regression:

Authorities should, at a minimum, have access to TR-held data where that data can also be received directly from an entity.

The ability to access OTCD data held in TRs represents a significant change from the methods authorities have traditionally used to access information related to OTCD transactions. Access to TR-held data will enable authorities to move from decentralised access to information (directly from reporting entities or from each other) to a more centralised access (through TRs that collect and store data from

reporting entities and facilitate access by authorities to that data). Therefore, authorities that need to access TR-held data in order to carry out their mandate(s) should be able to access, at a minimum, the same level of detail as they would receive directly from reporting entities. For example, where an authority can request, through its mandate, all transaction-level data from a given dealer, then at a minimum that authority would typically require access to all transaction-level data held at TRs where that dealer is one of the counterparties. Authorities should also be able to access such data in at least as timely a fashion as had they collected it directly from the regulated entity (there should be no additional delay in access to that data by using a TR).

Similarly, where data are reported to a TR in order to satisfy an authority's OTCD reporting requirement, that authority should be able to access that data in the TR.

Responsibility for approving access

In compliance with applicable laws and based upon the guidance provided in this report, a TR is expected to make a judgment whether the application of the requesting authority is consistent with its mandate. Authorities should support their requests for data by providing sufficient information to TRs on the basis for their mandate. In very exceptional cases, the TR supervisor may get involved in assisting to complete the initial determination for data access by a requesting authority.

Prior to an authority's first data request, a first determination will need to be done to evaluate the depth, breadth and identity parameters that will be granted to the authority to access the data held by the TR.[52] A second step, once the requesting authority is granted access to the data by the TR and standard reports of information are given, will be the determination to evaluate the validity of the requesting authority to data either for a mandate not included in this report or for data going beyond the typical depth, breadth or identity as defined by this report.

In compliance with applicable laws and based upon the guidance provided in this report, the TR would be expected to make a judgment whether the application of the requesting authority is consistent with its mandate (using the mapping table to assess typical requests, as well as supporting recommendations, access guidelines and guidance in the case of non-typical requests). This approach is not intended to require the TR to perform an independent assessment of the scope of the mandate (eg through a legal opinion), which could cause unnecessary delay in making the determination on a request for data.

The requesting authority would be expected to facilitate this decision-making process by providing the TR with sufficient information regarding the legal, regulatory or other relevant basis for its mandate(s) and a description of how the data request is necessary in order for the requesting authority to satisfy its mandate(s). An illustrative template of the type of information expected from an authority in support of its first request under a mandate or for any non-typical request is provided in Annex A.

In the very exceptional cases where this process may not be sufficient to reach a common view between the TR and the requesting authority, the TR supervisor may get involved in assisting to identify which authorities may receive information from a TR based on their mandate(s) (initial determination). However, the TR supervisor is not expected to be involved in validating typical individual data requests from those authorities. Consistently with the CPSS/IOSCO Responsibility E, and depending on the applicable legal framework and on the cooperative oversight and supervisory arrangements for the TR,

[52] Some jurisdictions may require preliminary steps for an authority to gain access to TR data (such as a cooperation agreement or an appropriateness determination).

the TR supervisor should coordinate with other relevant authorities that have regulatory, supervisory, or oversight responsibilities vis-à-vis the TR.[53]

6 Typical data access mapping

6.1 Introductory remarks

The following table summarises the minimum typical data access levels for each mandate discussed in Section 3. This data access mapping is based on the supporting recommendations and guidelines described in Section 5 above and reflects the analysis in Section 3 of the typical data access needs arising from each of the identified mandates.

The table is not intended to limit the information that can be made available to authorities, but represents the minimum set of information that should be made available to them. The table reflects the most granular information that could be typically expected to be accessed for a particular functional mandate but the table does not intend to imply that each authority requesting data under a given mandate would necessarily request all the data available for that authority.

This mapping of data is intended to reduce the discretion of TRs in assessing data requests from interested authorities, and it illustrates the minimum level of access that TRs make available to requesting authorities, based on the mandate(s) of the requesting authority.

TRs also should maintain flexibility in responding to requests for data in which the authority has an interest arising from its mandate but that may fall outside the scope of this table. In these circumstances, local law may provide that the TR or the TR supervisor has a role in determining the appropriateness of this request, and accordingly ensuring that the information requested arises from the mandate(s) of the requesting authority (either by ensuring the TR provides access to the information or by receiving and transmitting the information to the requesting authority).[54]

Authorities that wish to gain a broader view of the network across jurisdictional borders should have the option of seeking agreements with other jurisdictions on reciprocal data sharing.

Finally access to more granular information should not prevent an authority from also having access to aggregated information based on the more granular information (for example, access to transaction-level information should also allow for position-level and aggregate-level information based on this information).

[53] A cooperative arrangement between the TR supervisor and requesting authorities may cover how to answer non typical data requests.

[54] Some TR supervisors may not give guidance, ex-ante, to a TR when the TR is doubtful about the appropriateness of a data request, but would review ex-post any decision by the TR in light of its responsibilities as a TR supervisor.

6.2 Table

	Assessing systemic risk (examining size, concentration, interconnectedness, structure)	Evaluating derivatives for mandatory clearing determinations and monitoring compliance with such determinations	Evaluating derivatives for mandatory trading determinations and monitoring compliance with such determinations	General macro assessment	Conducting market surveillance and enforcement
Definition	An authority with a mandate to monitor a financial system and to identify emerging risks	An authority that has a mandate to evaluate OTCD for mandatory clearing determinations and monitoring its implementation	An authority that has a mandate to evaluate OTCD for mandatory trading determinations and monitoring its implementation	An entity that has a mandate to foster and support financial stability globally	An authority that has a mandate to conduct market surveillance and enforcement
Typical depth of data required	Transaction-level	Transaction-level	Transaction-level	Position-level	Transaction-level
Typical breadth of data required	All counterparties	(1) Any transactions in which one of the counterparties is within its legal jurisdiction and (2) all transactions on the underliers (i) within its legal jurisdiction (whether the counterparties are in the jurisdiction or not), (ii) for which the authority considers making or makes a mandatory clearing determination, or (iii) any transactions involving the same type of OTCD contract as the one being evaluated (whether the counterparties or underliers are in the jurisdiction or not)	(1) Any transactions in which one of the counterparties is within its legal jurisdiction and all (2) transactions on the underliers (i) within its legal jurisdiction (whether the counterparties are in the jurisdiction or not) or (ii) for which the authority must make a mandatory trading determination	All counterparties	Any transactions for counterparties in its legal jurisdiction as well as branches or subsidiaries of these counterparties which may be in other jurisdictions, and all transactions on the underliers within its legal jurisdiction (whether the counterparties are in the jurisdiction or not)
Identity	Named data for counterparties and underliers within their legal jurisdiction. Anonymised data for other counterparties	Anonymised counterparties and named data where named data are required for evaluating determinations; named data for monitoring compliance with such determinations	Anonymised counterparties and named data where named data are required for evaluating determinations; named data for monitoring compliance with such determinations	Anonymised	Named data

	Registering and regulating market participants and supervising market participants with respect to business conduct and compliance with regulatory requirements	Prudentially supervising financial institutions	Supervising/ overseeing exchanges, organised markets and organised trading platforms	Regulating, overseeing and supervising payment or settlement systems	Regulating, overseeing and supervising CCPs	Regulating, overseeing and supervising TRs
Definition	An authority that has a mandate to supervise market participants.	An authority that has a mandate to supervise and regulate or to monitor and conduct surveillance on the financial institution	An authority that has a mandate to supervise exchanges, organised markets and organised trading platforms	An authority that has a mandate to oversee a payment or a settlement system	An authority that has a mandate to supervise or oversee a CCP	An authority that has a mandate to supervise a TR
Typical depth of data required	Transaction-level	Transaction-level	Transaction-level	Transaction-level	Transaction-level	Transaction-level
Typical breadth of data required	Transactions in which one of the counterparties, whether registered or not, is within its legal jurisdiction, or in which one of the counterparties engages in OTCD transactions with, or whose OTCD transactions are guaranteed by, an entity within its legal jurisdiction (whether the counterparties are in the jurisdiction or not)	Transactions in which one of the counterparties is a consolidated organisation whose parent is supervised by the authority, including all subsidiaries, domestic or foreign, of the entity	Any transactions traded on an exchange, organised market or organised trading platform supervised by the authority	Any transactions settled by a payment or settlement system overseen by the authority	Any transactions that are cleared by a CCP supervised or overseen by the authority	Any transactions reported to the TR
Identity	Named data	Named data	Named data	Anonymised transaction-level data as a general rule, but named position-level data for the counterparties of the central bank and where investigation of suspicious activity is needed.	Named data	Named data

	Planning and conducting resolution activities	Managing currency policy	Implementing monetary policy	Lender of last resort function
Definition	An authority that has a mandate to resolve financial institutions	An authority in its function as monetary policy authority	An authority in its function to implement monetary policy	An authority in its function as possible lender of last resort
Typical depth of data required	Transaction-level	Transaction-level (Participants within legal jurisdiction), aggregate-level (all participants for underliers denominated in its currency)	Aggregate-level	Position-level
Typical breadth of data required	Any transactions in which one of the counterparties is the entity subject to resolution or a domestic or foreign affiliate	Any transactions that specify settlement in that currency, including transactions for which that currency is one of two or more specified settlement currencies	Any transactions for participants within a central bank's legal jurisdiction or underliers denominated in a currency for which the central bank is the issuer	Any transactions for which a named institution is a counterparty
Identity	Named data	Anonymised	Anonymised	Named data

Annex A: Illustrative template for Data Request Form

I. General Information	
Full name of requesting authority	
Country of origin	
Type of authority	
Contact details Main liaison (name / function / phone no./ email address	

List of personnel requesting accreditation			
Name	Function	Phone number	Email address

II. Context of the request and mandate
Please indicate each of the mandates that in your view allow you access to data and the relation between such mandate and the data requested.
III. Relevant basis to support the request
Please describe the legislative, regulatory or other relevant basis for your data request for each functional mandate listed above. Please provide supporting documentation, links, or other information to support the request, ideally in a language commonly used in the international derivatives markets
IV. Confidential treatment of data
Please confirm you have the authority and ability to keep the data confidential.
V. Description of requested data
Please describe in the most accurate way possible your request for data.

Annex B: Glossary of terms

Term[55]	Definition
Aggregate-level:	An authority may view both gross and netted data attributable to all participants that may be summed using various categories, including by product, currency, region, underlier etc that are not specific to any uniquely identifiable participant or transaction.
Authorities	The term "authorities" is intended to encompass, at a minimum, public sector authorities including central banks, securities and market regulators, prudential supervisors of market participants, resolution authorities and other authorities that would have a material interest in OTC derivatives data in furtherance of their responsibilities. In some instances, law enforcement authorities may also have a legal right to access data from trade repositories.
Central Counterparty*	An entity that interposes itself between counterparties to contracts traded in one or more financial markets, becoming the buyer to every seller and the seller to every buyer and thereby ensuring the performance of open contracts.
Collateral*	An asset of third-party commitment that is used by a collateral provider to secure an obligation vis-à-vis a collateral taker.
Counterparty	A party to an OTC derivatives trade
Derivative*	A financial contract whose value depends on the value of one or more underlying reference assets, rates or indices, on a measure of economic value or on factual events.
Financial market infrastructure*	A multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions
Jurisdiction	For the purpose of this report, except where "legal jurisdiction" is explicitly mentioned, jurisdiction refers to the geographical territory of a public authority and not to the particular legal scope of the mandate, which could provide effects in different countries or regions.
Legal risk*	The risk of the unexpected application of a law or regulation, usually resulting in a loss.
Mark-to-market*	The practice of revaluing securities and financial instruments using current market prices.

[55] The terms followed by an asterisk are copied from the CPSS-IOSCO PFMI published 16 April 2012.

Notional amount[56]	Total currency amount or total quantity in the unit of measure of an underlying commodity.
Position-level	An authority may view data reflecting both the gross and netted open positions that are specific to a) a uniquely identifiable participant or b) for a particular OTCD product or asset class (a set of transactions pertinent to a pair of participants). Position-level data are a snapshot at a point in time of all open positions for a particular product or type of products or for a given counterparty or group of counterparties. Unlike transaction-level data, this aggregation level does not include data reflecting the details of individual transactions, but the summing of one or more transactions will provide position information for one or more counterparties at a point in time.
Systemic risk	Systemic risk refers to the potential that an event, action, or series of events or actions will have a widespread adverse effect on the financial system and, in consequence, on the economy.
Trade repository*	A trade repository is an entity that maintains a centralised electronic record (database) of transaction data.
Transaction-level	An authority may view data that are specific to uniquely identifiable participants and transactions. A transaction represents a single economic relation between two counterparties, defined by a contract. A transaction record typically specifies a) the contract terms and b) both counterparties to the contract.
Typical access	Typical access refers to the minimum expected access requirements under a particular mandate as currently understood and as set forth in this report.
Non-typical access	A non-typical request refers to (i) requests for other types of data than suggested by the mandate of the authority, (ii) a request for access to data coming from an authority with a functional mandate that has not been listed under the guidance set in this report.
Underlier	That which the value and cash flows or deliverables under a derivative transaction are calculated, such as an asset, basket of assets, index, rate or derivative.

[56] This term is copied from the Data Report published in January 2012.

Annex C:
Members of the CPSS-IOSCO WG on TR data access by authorities

Working group co-chairs

Banque de France	Frédéric Hervo
Autorité des marchés financiers (Québec)	Derek West

Members

Australia Securities and Investment Commission	Damien Scholefield
National Bank of Belgium	Steven Van Cauwenberge
Comissão de Valores Mobiliários (Brazil)	Sérgio Schreiner
European Central Bank	Patrick Foell
European Securities and Markets Authority	Frederico Alcântara de Melo
Autorité des marchés financiers (France)	Julien Jardelot
Bundesanstalt für Finanzdienstleistungsaufsicht (Bafin)	Christian Schindler
Deutsche Bundesbank	Anna Pliquett
Hong Kong Monetary Authority	Colin Hak Wan Pou
Securities and Futures Commission (Hong Kong)	Daphne Doo
Banca d'Italia	Barbara Lupi
Bank of Japan	Akiko Kobayashi
Financial Services Agency (Japan)	Jutaro Kaneko
Bank of Korea	Kwangsok Choi
Banco de México	Luis Manuel de los Santos
Ontario Securities Commission	Kevin Fine
Monetary Authority of Singapore	Kenneth Bing Yong Gay
Comisión Nacional del Mercado de Valores (Spain)	Miguel Angel Herrero Alvite
Bank of England	Anne Wetherilt
Financial Conduct Authority (UK)	John Tanner
Board of Governors of the Federal Reserve System	Jennifer Lucier
Federal Reserve Bank of New York	Marsha Takagi
Commodity Futures Trading Commission	Warren Gorlick
U.S. Securities and Exchange Commission	Richard Gabbert

Observers

Finansinspektionen (Sweden, rep. ODRF)	Jan Axelsson
Federal Deposit Insurance Corporation (rep. ODSG)	John Feid
European Commission	Muriel Jakubowicz
International Monetary Fund	John Kiff

Basel Committee on Banking Supervision	Nayef Alsadoun
Secretariat	
CPSS	Angela O'Connor
IOSCO	Yukako Fujioka

The report also benefited from contributions from Fabrizio Planta (European Securities and Markets Authority), Aaron Unterman (Ontario Securities Commission, Canada), Junko Miyazaki and Hiroyuki Nishizawa (Bank of Japan), Ana Lasaosa (Bank of England), Robert Barnes and Stephen Longden (Financial Services Authority, UK), Mauricio Melara (Commodity Futures Trading Commission, U.S.), Shari Bower (Federal Reserve Bank of New York), Namirembe Mukasa (Board of Governors of the Federal Reserve System), and Kim Allen and Katherine Martin (U.S. Securities and Exchange Commission).

The co-chairs would like to give thanks to Alexis Jordan and Laurent Kersenbaume (Banque de France) and Jean-Philip Villeneuve (Autorité des marchés financiers, Québec, Canada) for their participation in the drafting of the report.