June 21, 2013

Mr. Richard Shilts
Director
Division of Market Oversight
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, N.W.
Washington, DC 20581

Re: Request for No-Action Relief – Parts 20, 45 and 46

Dear Mr. Shilts:

The International Swaps and Derivatives Association, Inc. ("**ISDA**"), on behalf of its members with reporting obligations under Part 20, Part 45 or Part 46 of the Regulations (collectively, the "**Reporting Rules**")[1] of the Commodity Futures Trading Commission (the "**Commission**") and other similarly situated persons, is writing to request, pursuant to Rule 140.99, an extension of the expiration date for the no-action relief provided under CFTC Letter No. 12-46, as described below.

ISDA's mission is to foster safe and efficient derivatives markets to facilitate effective risk management for all users of derivative products. ISDA has more than 800 members from 58 countries on six continents. These members include a broad range of OTC derivatives market participants: global, international and regional banks, asset managers, energy and commodities firms, government and supranational entities, insurers and diversified financial institutions, corporations, law firms, exchanges, clearinghouses and other service providers.

In December 2012, the Commission's Division of Market Oversight ("**DMO**") issued CFTC Letter No. 12-46 in response to a request from ISDA expressing concern regarding conflicts between the privacy laws of non-US jurisdictions and the Reporting Rules. CFTC Letter No. 12-46 granted conditional and time-limited no-action relief that permits a reporting party to omit from reports made pursuant to the Reporting Rules the non-reporting party's LEI, the identity of the non-reporting party in specifically enumerated data fields and certain other terms that the reporting party reasonably believes would identify the non-reporting party (the information that may be omitted, "**Identity Information**"). In addition, the relief permits a reporting party to temporarily withhold reporting of Rule 45.3 confirmation images that include the covered Identity Information and would otherwise need to be manually redacted. The relief granted in CFTC Letter No. 12-46 expires on the earlier of (i) the reporting party's obtaining counterparty consent or regulatory authorization, as applicable, (ii) the reporting party no longer holding the

[1] The relief requested in this letter also encompasses CFTC Rules 23.204 and 23.205 insofar as the swap entity has complied with the conditions of the no-action relief with respect to the reporting required under such rules.

requisite reasonable belief regarding the privacy law consequences of reporting or (iii) 12:01 a.m. eastern daylight time on June 30, 2013.

ISDA requests that DMO extend the expiration date for the relief granted under CFTC Letter No. 12-46 with respect to reportable transactions for which the reporting of Identity Information is subject to statutory or regulatory prohibitions of one of the non-U.S. jurisdictions listed in the Annex (each, an "**Enumerated Jurisdiction**")[2] until the earlier of (i) the reporting party no longer holding the requisite reasonable belief regarding the privacy law consequences of reporting or (ii) 12:01 a.m. eastern daylight time on June 30, 2014.[3]

Based upon advice obtained by ISDA members, the Enumerated Jurisdictions fall into two categories: (i) those for which non-reporting party consent is not a viable solution to privacy law conflicts due to the legal requirements such consent must satisfy and (ii) those for which non-reporting party consent alone is not effective and regulatory authorization that would permit the reporting of Identity Information has not been available to affected market participants.

We note that the local law advice received by various ISDA member firms is not uniform. The differences in advice underscore the complexity and novelty of the issues the industry is now facing. While consensus generally exists around a majority of the "problematic jurisdictions", even competent counsel in each jurisdiction can have differing views as to the cross-border reach of local law and the effectiveness of consent. We note also that the laws in many jurisdictions apply differently based on an institution's presence in a given jurisdiction. What is a problematic jurisdiction for one member, therefore, is not for another. The purpose of this letter is to identify and seek relief for jurisdictions in which member firms reasonably believe that a standing blanket counterparty consent is insufficient to overcome relevant local data privacy concerns.

With respect to Enumerated Jurisdictions in the first category specified above, concerns include, for example, the revocability of consents, requirements that specific consent be given for each instance of disclosure, and legal standards that expose dealers to unacceptable risk that consent may later be found to be ineffective. Although the laws of certain Enumerated Jurisdictions would recognize consent given on a transaction-by-transaction basis, this means of overcoming privacy conflicts appears to be of limited practical utility. In a voice trading environment, questions remain as to whether oral consent is legally effective and whether the trading personnel with whom a firm interacts directly are authorized to provide it. Further, reliably controlling for and cataloguing such oral consent is difficult and would expose firms to operational and legal risks. With respect to electronic trading, the industry has had insufficient time to develop

[2] An Annex listing the Enumerated Jurisdictions, and describing briefly the applicable privacy law restrictions, is attached hereto. The Annex descriptions should be regarded as reasoned views of the operation of the cited provisions in the novel context of SDR reporting. An analysis of conflicts questions with regard to the disclosure of counterparty information for other regulatory purposes could yield different results. Accordingly, the list should not be regarded as a final and conclusive list of problematic jurisdictions. Industry participants have prioritized their review of international jurisdictions by relevance, and this list therefore includes jurisdictions in addition to those identified as problematic in ISDA's request for the relief granted in CFTC Letter No. 12-46. While reflective of the collective knowledge to date of ISDA members that have provided information, the list is not necessarily comprehensive.

[3] ISDA expects to submit a separate request letter addressing the practical difficulties of obtaining non-reporting party consent.

functionality for obtaining "click through" consents at the time of trade. Much electronic trading occurs through third-party information and communication services, whose cooperation would be required to develop such means of consent. Moreover, click-through consents could not be utilized in the case of automated trading, where there is no human interface.

With respect to Enumerated Jurisdictions in the second category, ISDA members have not identified any practicable means of resolving the conflict of laws short of statutory or regulatory changes in those jurisdictions. The issue of conflicts with privacy laws and blocking statutes has been recognized by international regulators as one of the implementation challenges for trade reporting, and dialogue is taking place to seek a resolution.[4]

Reporting party behavior in accordance with CFTC Letter No. 12-46 achieves substantially complete compliance with the Reporting Rules even after the omission of Identity Information from Part 20, 45 and 46 reports. Unless the relief with respect to Enumerated Jurisdictions is extended beyond June 30, registered swap dealers may not be able to continue participating in these markets, with concomitant negative impact on both the local markets and Commission registrants. Deferring the expiration date of the relief as requested would avoid this undesirable outcome and allow time for the affected jurisdictions to resolve cross-border conflicts associated with swap data reporting, an issue now prominently on the international regulatory agenda, as they implement their own data reporting frameworks. Accordingly, the requested relief is an appropriate extension of comity to these non-US jurisdictions, without detracting from the Commission's ability to achieve its objectives under the Reporting Rules.

For the foregoing reasons, ISDA requests that the staff of the Division of Market Oversight issue the no-action relief described above.

Thank you for your consideration of these concerns. Please contact me or ISDA staff if you have any questions or concerns.

Sincerely,

Robert Pickel

[4] See, e.g., OTC Derivatives Market Reforms – Fifth Progress Report, Financial Stability Board (April 2013), pp.48-49 ("authorities reported that plans to adopt legislation and/or regulation that would allow for such reporting are underway ") (available at http://www.financialstabilityboard.org/publications/r_130415.pdf).

ANNEX

Enumerated Jurisdictions – summary of privacy restrictions

i. France

Trade Participants may only disclose Trade Data involving a counterparty if the disclosure is made: (i) pursuant to a list of statutory exemptions or (ii) the counterparty delivers its consent to the disclosing Trade Participant each time the latter intends to make a disclosure. Relevant provisions of French law include: (i) Article L. 511-33 et seq. of the French Code monétaire et financier for credit institutions and (ii) Article L. 531-12 et seq. of the same code for investment firms.

Trade Data reporting to SDRs may not qualify for any statutory exemption and transaction-by-transaction consent is not a feasible solution for high-volume activity and would certainly result in delayed reporting. Consent that is to be obtained via an industry protocol such as the ISDA August 2012 Dodd Frank Protocol or via a single side letter may not be sufficient for this reason. Requests for disclosure by foreign legal or regulatory authorities—without instruction from a French authority—are similarly insufficient. Potential liabilities for violations of local privacy law in France include fines of up to €75,000 for legal persons and €15,000 for natural persons, action for damages, suspension of operations, withdrawal of business licenses and, for natural persons involved in a violation, imprisonment of up to one year.

The French blocking statute (Law 68-678 of 26 July 1968) applies to any person / entity located in France, or even located outside of France, when there is an action taken with the purpose to obtain from a French company or individual any information which is economic, commercial, industrial, financial or technical nature tending to constitute evidence in view of foreign judicial or administrative proceedings or in the framework of such proceedings, even if such disclosure is made with the approval of the relevant counterparty.

ii. Korea

Trade Participants may not be able to disclose any Trade Data about their respective counterparties unless the disclosures in question are made at the order of Korean regulators, the Financial Services Commission or Governor of the Financial Supervisory Service or otherwise qualify for an exemption under the Real Name Act. Relevant provisions of the Real Name Act include: (i) Article 3 and (ii) Article 4.1. Disclosures which include personal data relating to natural persons are also governed by the Personal Information Protection Law.

Written consent may also need to be obtained each time disclosure is sought. Accordingly, the use of an industry protocol to report Trade Data, or consent via a side letter, would not satisfy the statute's requirements. Members have been informed that the Financial Services Commission has indicated that broad consent provisions granting consent for all future transactions would not meet the requirements of the Real Names Act. Further the obligations of confidentiality under the Real Names Act cannot be excluded through contractual terms. There are limited exceptions to the Real Names Act which permit disclosure in the absence of client consent but these are not applicable. Disclosures made upon the request of foreign legal or regulatory authorities would

similarly be in violation of local law. Violations of local law in Korea under the Real Name Act can trigger fines of up to 100 million Korean won and, for natural persons, imprisonment of up to five years. Under the Capital Market Act, fines can range up to 200 million Korean won and imprisonment of natural persons for five years. The Personal Information Protection Law has very specific consent requirements which include an obligation to inform the data subject of the disadvantages of granting consent, and failure to comply with the statute may result in imprisonment of up to five years or a fine.

iii. Luxembourg

Trade Participants may not be able to disclose Trade Data unless the relevant disclosure requirement is under applicable local law. Luxembourg requires that any consent delivered by a counterparty must satisfy the standards set forth by Luxembourg's Comité des juristes (the "**CODEJU**"), which is an advising committee of the Luxembourg finance sector regulator, the Commission de Surveillance du Secteur Financier. Relevant provisions of Luxembourg law include: (i) Articles 37-1(1), 41(1) through (5bis) of the Luxembourg law of 5 April 1993 on the financial sector and (ii) Articles 111-1(2) to 111-1(8) of the law of 6 December 1991 on the insurance sector.

A counterparty's consent to disclosure of Trade Data to an SDR may not be covered by a statutory exemption and the use of an industry protocol to deliver consent may not satisfy the CODEJU's standards. Disclosures made upon the request of foreign legal or regulatory authorities may also not qualify for a statutory exemption nor satisfy the CODEJU standards. The CODEJU's standards may include the requirement for such consent to be revocable (as a matter of public policy) and to relate to a disclosure which is in the best interests of the consenting party. Furthermore, the consent must be specific as to the information that may be disclosed, the identity of the person to whom the information may be disclosed, the intended aim of the disclosure, and the time period for which the consent is valid. Violations of Luxembourg law can trigger a range of penalties, including fines of up to €5,000 for natural persons and €10,000 for legal persons, contractual damages, injunction orders, withdrawal of licenses, suspension or prohibition of business activities, professional bans and imprisonment of natural persons for a period of up to six months.

iv. People's Republic of China

Trade Participants may disclose Trade Data at the instruction of the Chinese regulatory authorities pursuant to the state's Regulations on Financial Institutions" Anti-money Laundering. Trade Participants may also make disclosures as required by a foreign legal or regulatory authority, *provided* that local law permits the disclosure or the disclosure requirement is otherwise consistent with local law—which arguably would not be the case for disclosure of Trade Data under the Reporting Rules as there is no direct local equivalent. To the extent that Chinese law does not authorize disclosure of Trade Data, Trade Participants subject to such law would not be permitted to make any disclosures, regardless of a foreign law requirement or the consent of a counterparty. Potential liabilities for violation of Chinese privacy law include fines of up to RMB 500,000, suspension of operations and withdrawal of business licenses.

There is a prohibition on the disclosure of State Secrets (Law of the PRC on the Preservation of State Secrets effective October 1st 2010) and the definition of State Secrets is wide: " any information concerning national security and interest which, once disclosed, may impair the security and interest in the areas of politics, economy and national defence". Consent of a client will not overcome this prohibition.

Additionally, the Notice on Protection of Personal Financial Information by Banking Financial Institutions published by the Peoples Bank of China prohibits the disclosure of Personal Financial Information to foreign institutions. Personal Financial Information includes any information regarding an individual's identification, assets, credit status, financial transactions and even information derived from processing or analysing the individual's consumption habits or investment intention. The only exception to this is where the local banking branch needs to provide the Personal Financial Information to overseas affiliates in order to provide the services and further that the client has consented to the disclosure. Such exception does not apply in the present circumstances.

v. Switzerland

Swiss privacy rules, such as Article 47 of the Swiss Federal Act on Banks and Saving Institutions of 8 November 1934 (the "**Swiss Banking Act**"), prohibit banks from disclosing any client information to any third party. Additionally, under Swiss data protection law, the transfer of any personal data of third parties abroad is closely restricted and requires, inter alia, the relevant person's consent. This prohibition includes client and employee information. Under Article 271, any action undertaken for a foreign authority is prohibited if the action undertaken in Switzerland is by its nature an official or sovereign act whose performance is reserved to a Swiss authority and is performed without the involvement or authorization of the competent Swiss authority, irrespective of whether the action is undertaken by a private person or directly by the foreign authority.

Article 271 separately prohibits the facilitation of any action, such as disclosure of restricted information, undertaken in the interest of a foreign authority, if such action is considered under Swiss law an act that would have to be undertaken by a competent Swiss authority. In relation to financial institutions, the Federal Finance Department ("**FFD**") is authorized to provide an exemption under Article 271 to permit disclosure of client information. The FFD may submit the case to the Swiss Federal Government. In taking its decision, the Swiss Federal Government will weigh the public and private interests involved, particularly the protection and safeguarding of the rights of third parties (e.g., clients and employees). Penalties for violations of Article 271 include significant fines and imprisonment of up to three years for any natural person violating the law.

vi. Taiwan

Under Article 48 of the Taiwan Banking Act, licensed banks in Taiwan must keep counterparties' information confidential unless the disclosure is permitted by the laws or regulations of Taiwan or is otherwise "stipulated" by the Taiwan Financial Supervisory Commission ("**Taiwan FSC**"). Guidance issued by the Taiwan FSC expressly permits banks to release the counterparty data to (i) Taiwanese agencies (e.g., tax authorities, prosecutor offices),

(ii) home country regulators of a Taiwan branch of a foreign bank pursuant to home country regulation or (iii) approved outsourcing service providers. Thus, for a non-U.S. bank branch, swap data reporting to a CFTC-registered SDR does not fall into any of the current exemptions. Penalties for violations may include administrative fines, damages, and potential criminal liability if the disclosed information is considered a "business secret."

vii. Belgium

To the extent that Identity Information includes Personal Data (meaning any information relating to an identified or identifiable natural person), consent of the data subject will not be effective to overcome the restrictions. The Act of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data, as amended by the Act of 11 December 1998 and the Act of 29 February 2003, as well as supplemented by the Royal Decree of 13 February 2001 (the "**Data Protection Act**") governs the disclosure of such personal data.

The Data Protection Act prohibits transfer of data to U.S authorities and the view is that such a transfer is illegal and cannot be legalized by consent of the data subject (Article 29 Working Party Opinion 15/2011 of 13 July 2011 and also Council Decision 2010/412/EU of 13 July 2010).

viii. India

The Reserve Bank of India ("**RBI**") sets out confidentiality obligations of a bank toward its clients in its Master Circular on Customer Service in Banks, which provides that:

The scope of the secrecy law in India has generally followed the common law principles based on implied contract. The bankers' obligation to maintain secrecy arises out of the contractual relationship between the banker and customer, and as such no information should be divulged to third parties except under circumstances which are well defined. The following exceptions to the said rule are normally accepted:

(i) Where disclosure is under compulsion of Indian law;
(ii) Where there is duty to the public to disclose;
(iii) Where interest of bank requires disclosure; and
(iv) Where the disclosure is made with the express or implied consent of the customer.

However, there is no specific provision in the RBI's regulatory circulars permitting reporting of data pertaining to Indian banks or branches to non-Indian regulators. In a circular relating to retention of data offshore, the RBI has stated that non-Indian regulators should not have access to Indian branch data stored overseas. The RBI has advised member firms operating in India that prior approval must be obtained from the RBI in order to report or disclose branch information to the CFTC. The RBI's position prohibits any reporting of transactions booked in a firm's Mumbai branch to an SDR located outside of India, notwithstanding clauses (i) and (iii) referenced immediately above.

Thus, absent affirmative consent from the RBI and customer consent, a firm cannot report swaps booked in its Mumbai branch, even with counterparty-identifying information redacted.

ix. Algeria

Reporting to an SDR may implicate Algerian bank secrecy rules under Article 117 of Ordinance 03-11 of 26 August 2003 on the currency and credit.

Professional secrecy obligations under penalty of sanctions under the criminal code are binding on:

- any member of a Board of Directors, any external auditor and any person who participates or has participated to the management of a bank or financial institution or who is or was employed by them; and
- any person who participates or who participated in the control of banks and financial institutions.

Subject to the express provisions of law, the bank secrecy is enforceable against all authorities except:

- towards the public authorities which appoint administrators of banks and financial institutions
- towards the judicial authority acting in the framework of criminal procedures;
- towards the public authorities required to communicate information to international institutions entitled, particularly in the context of the fight against corruption, money-laundering and the financing of terrorism;
- towards the Bank of Algeria or the banking committee at the bank of Algeria, which may transmit information to the authorities responsible for the supervision of banks and financial institutions in other countries, subject to reciprocity and provided that these authorities are subject to the professional secrecy with the same guarantees as in Algeria.

x. Singapore

Trade Participants may only be entitled to disclose Trade Data to local regulatory authorities as required by Singapore law. Under Regulation 47(2) of the Securities and Futures (Licensing and Conduct of Business) statute (the "**SFR**"), Trade Data may only be able to be disclosed at the instruction of the Monetary Authority of Singapore (the "**MAS**"). Therefore, many Trade Participants may not be able to disclose Trade Data at the request or demand for disclosure by a foreign authority or an SDR unless such disclosure has been otherwise authorized by the MAS—even upon the consent of the applicable counterparty. Trade Participants' accession to an industry protocol that contains provisions to obtain consent to disclose Trade Data may not be effective absent approval of the MAS. Although firms have received indications that such approval may be forthcoming, some firms are continuing to redact Identity Information until such time as the MAS may make an official public announcement.

Violations of Singapore privacy law can trigger civil and criminal liabilities, including fines (up to $S125,000 for natural persons and $S250,000 for legal persons), damages in tort, revocations of licenses and imprisonment of up to three years for natural persons.

xi. Bahrain

If a firm has a local office or presence or conducts data collection in Bahrain, consent is not effective. If no swap dealer office or presence in the jurisdiction, reporting is permitted. In the former instance, exploitation or misuse of personal information is governed by Art.l58 of the Civil Code of Bahrain. If a reporting party was considered negligent in transferring data and if the individual suffered damage as a result of the transfer damages apply.

xii. Argentina

Local laws should not apply if the reporting party has no Local Presence. The Financial Entities Law 21,526 (the "**FEL**") applies to activities performed in Argentina. In addition, the Personal Data Protection Law 25,326, as amended (the "**PDPL**"), applies to databases or registries that include personal data. Although the law makes no express reference to location, provisions in principle apply to databases located in Argentina.

Data Regulations which prohibit or restrict the disclosure of Data to an SDR.

(i) the FEL, and

(ii) the PDPL.

The FEL prohibits Financial Entities to disclose information on transactions carried out for, or data received from, their customers. This prohibition is, however, limited to transactions that are registered as "Liabilities" in the financial statements of the Financial Entity. Additionally, the Financial Entities have no duty of confidentiality regarding those operations registered as "off-balance sheet" activities, such as securities custody services. Despite the foregoing, certain government agencies, including the tax authorities, anti-money laundering agencies and the Central Bank of the Republic of Argentina (the "**CBRA**"), may require Financial Entities to disclose such information. The above mentioned prohibition does not apply to customers of a Financial Entity, who have full access to their own information, nor to the agents or representatives of the customers in their relationship with the Financial Entity. Legal commentators also include within this exception the employees of a customer, acting in the course of their employment for the customer. On the other hand, the PDPL provides that any information relating to and identified or identifiable individual –natural person or legal entity– is considered personal data ("**Personal Data**"). In addition, the PDPL states that Personal Data is subject to confidentiality obligations on the holder of such data.

Disclosure to the SDR or the CFTC-express consent of the swap counterparty.

The consent of the data owner is not included in the FEL among the exceptions to the confidentiality/secrecy obligation. Basically, exceptions relate to petition made by courts, tax

authorities and the CBRA. We understand however that if we were to assume that the confidentiality/secrecy obligation is aimed to protect the data owner's privacy right; then, as beneficiary of such right, the data owner should be able to waive it. On the contrary, it could be argued that the waiver of the confidentiality/secrecy obligation made by the data owner does not release the obligation imposed by the FEL. In this regard, the BCRA may not be opened to accept that the data owner has the authority to modify the content of the FEL; in other words, the BCRA may resolve that the Financial Institution is not released from the confidentiality/secrecy obligation even when the customer has authorized it to disclose information. Counsel not aware of judicial precedents, therefore it is difficult to predict how a court will resolve this conflict of different rights/obligations.

One of the exceptions to the confidentiality/secrecy obligation is where the Financial Entity obtained previous authorization from the BCRA to disclose certain information. Counsel believe that the Financial Entity could inform the BCRA the reasons why it needs to disclose certain information, explain that it has obtained the authorization of the data owner to disclose such information, and request the BCRA´s authorization. Under this scenario, BCRA may be willing to authorize the Financial Entity to disclose the information.

Potential criminal and civil penalties for non-compliance.

The Criminal Code, in Section 157 bis, provides that it shall be subject to imprisonment from one (1) month to two (2) years, the person which (i) knowingly or unlawfully, or in violation of confidentiality and data security systems, has access, in any way, to a personal database; or (ii) reveals to a third party information recorded in a personal database whose secrecy should be preserved as provided by law. In the event that the author is a public officer, an additional sentence of one (1) to four (4) years special disqualification shall apply. The FEL provides for different sanctions that may be applicable by the CBRA, including (a) warning, (b) fines, (c) suspension, or (d) revocation of the corresponding license. The PDPL in turn, provides for a number of sanctions of different types and degrees according to the seriousness of the offense incurred by the controllers or users of the databases. The Data Protection Authority, through its Regulation 1/2003 defined the offenses as serious and very serious. Administrative sanctions may include (a) warning, (b) suspension, (c) fines ranging between AR$1,000 (equivalent to US$200), and AR$100,000 (US$20,000); and (d) closure or cancellation of the file, register or database.

xiii. Hungary

Consent is not effective for Natural Person ECPs; Consent is effective for Corporate ECPs. Disclosure for Natural Person ECPs is not permissible without consent with full probative force as demonstrated by notary certifications and other formalities. Presence or local office implicates local statute and common law. Certain provisions of Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers and on the Regulations Governing their Activities (the "**Investment Services Act**") may be applicable to investment service providers which provide investment services in Hungary on a cross-border basis, even if such investment service provider does not have an office, or license, or personnel or representatives physically present in Hungary. Investment service providers that are registered in one of the European Economic

Community ("**EEC**") countries are entitled to provide investment services in Hungary on a cross border basis in accordance with the provisions of the Investment Services Act (based on Directive 2004/39/EC). In all other cases, a foreign investment service provider is entitled to provide investment services in Hungary only through its Hungarian registered and licensed subsidiary or branch office. Restrictions apply to disclosure of Data to the SDR.

Pursuant to Section *4 paragraph (2) and point 27 of the Investment Services Act*, "securities secrets" mean and includes all data and information that is at the disposal of an investment firm, an operator of multilateral trading facilities or a commodity dealer, concerning each specific client relating to its/his/her personal information, financial standing, business operations or investments, ownership or business relations, or its/his/her contracts or agreements with any investment firm or commodity dealer, or to the balance or money movements on its/his/her accounts. Said information qualifies as a "securities secret" irrespective of whether that information relates to (i) a human being, "Eligible Contract Participant ("**ECP**")", or (ii) an Institution, Corporation, Partnership, Hedge Fund or other type of non-human person.

Pursuant to *Section 118 (1) of the Investment Services Act*, investment firms and commodity dealers, and the executive officers and employees of investment firms and commodity dealers, and any other person affected, must keep confidential any securities secrets made known to them in any way, without any limitation in time.

Pursuant to *Section 118 (2) of the Investment Services Act*, investment firms and commodity dealers may disclose securities secrets to third parties, notifying the client affected, only if:

a) so requested by the client to whom the information pertains, or his legitimate representative, in an authentic instrument or in a private document with full probative force, expressly indicating the particular data, which are considered securities secrets, to be disclosed;
b) the regulations contained in Subsections (3)-(4) and (7) of section 118 the Investment Services Act, provide an exemption from the requirement of confidentiality concerning securities secrets; or
c) the disclosure is deemed necessary in light of the interests of the investment service provider or commodity dealer in selling its receivables due from the client or for the enforcement of its outstanding receivables.

Pursuant to *Section 118 (3) of the Investment Services Act*, the confidentiality requirement under *Section 118 (1) of the Investment Services Act* shall not apply to:

a) the Hungarian Financial Supervisory Authority, the Investor Protection Fund of Hungary, the National Deposit Insurance Fund of Hungary, the Hungarian National Bank, the State Audit Office and the Economic Competition Office of Hungary when acting within the scope of their powers and duties;
b) operators on the regulated markets, operators of multilateral trading facilities, bodies providing clearing or settlement services, the central depository, the Government oversight agency exercising its supervisory competence specified in Subsection (1) of Section 63 of the Act on State Budged Management, and the

European Anti-Fraud Office ("**OLAF**") monitoring the protection of the European Community's financial interests, when the above are acting within the scope of their duties conferred by law;

c) notaries public in connection with probate proceedings, and the guardian authority acting in an official capacity;
d) bankruptcy trustees, liquidators, financial trustees, bailiffs and receivers, in connection with bankruptcy proceedings, liquidation proceedings, judicial enforcement procedures, local government debt consolidation procedures, and in connection with a voluntary dissolution proceeding;
e) investigating authorities acting within the scope of criminal procedures in progress and when investigating charges, and the public prosecutor acting in an official capacity;
f) the court acting in criminal or civil cases, bankruptcy and liquidation proceedings and in the framework of local government debt consolidation procedures;
g) the agencies authorized to use secret service means and to conduct covert investigations if the conditions prescribed in specific other legislation are provided for;
h) the national security service acting within the scope of duties conferred upon it by law, based upon the special permission of the director-general;
i) tax authorities and the customs authorities in the framework of their procedures to monitor compliance with tax, customs and social security payment obligations, and for the implementation of an enforcement order issued for such debts;
j) the commissioner of fundamental rights when acting in an official capacity;
k) the Nemzeti Adatvédelmi és Információszabadság Hatóság (*National Authority for Data Protection and Freedom of Information*) acting in an official capacity;

when these bodies make written requests to the investment firm or commodity dealer concerned.

Pursuant to *Section 118 (4) of the Investment Services Act*, the confidentiality requirement under *Section 118 (1) of the Investment Services Act* shall not apply:

a) where the state tax authority makes a written request for information from an investment firm or commodity dealer on the strength of a written request made by a foreign tax authority pursuant to an international agreement, provided that the request contains a confidentiality clause signed by the foreign authority;
b) where the Hungarian Financial Supervisory Authority requests or supplies information in accordance with a cooperation agreement with a foreign supervisory authority, provided that the cooperation agreement or the foreign supervisory authority's request contains a signed confidentiality clause;
c) where the Hungarian law enforcement agency makes a written request for information from an investment firm or commodity dealer in order to fulfill the written requests made by a foreign law enforcement agency, provided that the request contains a confidentiality clause signed by that foreign law enforcement agency;
d) with respect to data supplied by the Investor Protection Fund of Hungary to foreign investor protection schemes and foreign supervisory authorities in the

manner specified in cooperation agreements if they guarantee equivalent or better legal protection for the processing and use of such data than the protection afforded under Hungarian law;

e) in respect of information provided by an investment firm or commodity dealer the Act on Tax Administration in relation to deceased persons.

Pursuant to *Section 118 (7) of the Investment Services Act*, the confidentiality requirement under *Section 118 (1) of the Investment Services Act* shall not apply where an investment firm or commodity dealer complies with the obligation of notification prescribed in the Act on the Implementation of Restrictive Measures Imposed by the European Union Relating to Liquid Assets and Other Financial Interests.

Disclosure to the SDR or the CFTC or other US regulator IS permissible with the express consent of the swap counterparty if the consent is provided in the appropriate form and is specific as to the information to be disclosed. Pursuant to Section 118 (2) of the Investment Services Act, investment firms and commodity dealers may disclose securities secrets to third parties, upon notifying the client affected, only if so requested by the client to whom the information pertains, or its/his/her legitimate representative in an authentic instrument or in a private document with full probative force, expressly indicating the particular data which is considered as a securities secrets and which may be disclosed.

Consent language is *not* sufficient to constitute express consent. Pursuant to Section 118 (2) of the Investment Services Act, the consent to disclose a securities secret(s) must expressly indicate the particular scope of the data which may be provided to the third party. Discussions with the relevant Hungarian regulators (the Hungarian Financial Supervisory Authority and the Data Protection Authority) would be required to determine whether the language contained in the 2012 ISDA Protocol would be considered as fulfilling the statutory requirement that the consent "expressly indicates the particular scope of the data" which otherwise constitutes a securities secret(s) and which may be disclosed. The express consent must be in an authentic instrument or in a private document with full probative force. Pursuant to Hungarian international private law and the Act III of 1952 on the Code of Civil Procedure (the "Civil Procedure Code"), if the ISDA agreement is duly signed by two legal entities, such agreement will qualify as a private document with full probative force. Pursuant to Civil Procedure Code, if the ISDA agreement is signed by an "Eligible Contract Participant (ECP)", such agreement will qualify as a private document with full probative force if:

a) the document is signed by two witnesses to verify that the document was transcribed by others and signed by the ECP in front of them, or that the signatory declared in front of the witnesses that the signature appearing on the document was the signatory's own. Said document must indicate the witnesses' permanent residence (home address) and signed and printed name as well;
b) the ECP's signature or initial has been certified on the document by a court or by a notary public;
c) an attorney (legal counsel) provides a document - duly signed by the attorney - to verify that the document was transcribed by others and signed by the ECP in front of him, or that the signatory declared the signature in front of the witness as being

the signatory's own, or that the electronic document executed by the ECP's certified electronic signature contains the same information as the electronic document made by the attorney;

d) the electronic document is executed by the ECP's certified electronic signature or advanced electronic signature attested by a qualified certificate.

Pursuant to Section 195 of the Civil Procedure Code, a paper-based or electronic document qualifies as an authentic instrument, if such document has been issued by a court, a notary public or another authority, or an administrative body within its sphere of authority, and in the prescribed form. Furthermore, a document recognized by another regulation as an authentic instrument shall also be deemed to have probative force.

- Potential criminal and civil penalties, where applicable, for non-compliance with each Data Regulation and/or common law obligation identified in 3(a) above (e.g., fines of [X] amount; imprisonment for [X] months, etc.).

  - fines from HUF 100,000 up to HUF 2,000,000,000 may be imposed by the Hungarian Financial Supervisory Authority;
  - imprisonment up to three years by the Hungarian criminal courts if the committing the crime of "breach of trade secret" (Criminal Code Section 300) is proved (in accordance with Hungarian criminal law / criminal procedure law);
  - civil law claim by the counterparty for damages and other legal remedy(ies) may be pursued before Hungarian civil courts on the basis of unpermitted discourse of data provided that the unpermitted disclosure and the amount of the damages caused by such disclosure are proved (in accordance with Hungarian civil law / civil procedure law); and
  - the Data Protection Authority my impose a fine of up to HUF 10 million if an inadequate level of information is provided to the data subject about the occurrence of the processing of his/her/its personal data. Both Hungarian Financial Supervisory Authority and Data Protection Authority are entitled to impose fines (based on different legal ground) and one authority imposing a fine does not prohibit the other authority to do the same. The above amounts of fines are the maximum amounts and the authorities have the right to determine the amount of the fine in each case based on their free evaluation of the facts and circumstances of the specific infringement.

xiv. Samoa

Data Regulations prohibit or restrict disclosure of Data to the SDR. The International Companies Act 1988, International Trusts Act 1988, International Partnership and Limited Partnership Act 1998 (ie legislation governing entities in Samoa's offshore or tax haven jurisdiction which can only operate outside of Samoa). Of these entities, by far the most common is an international company. There are very few international trusts, international partnerships and limited partnerships created in Samoa. There are no applicable Data Regulations for any other "domestic" (ie non-tax haven) entities incorporated and doing business in Samoa, or individuals

resident in Samoa. Disclosure is permitted for international companies, international partnerships and limited partnerships with express consent of an officer of the entity, subject to the proviso that the disclosure is not for compliance with a demand for information by a government, court or tribunal that will or is likely to result in the payment of any tax, penalty or fine. Disclosure is not permitted for international trusts. Potential criminal and civil penalties for non-compliance with each Data Regulation- For non-permitted disclosures relating to:

- International companies: criminal offence punishable by a maximum fine of WST50,000 (approx USD22,700) and/or 2 years imprisonment for the 1st offence; each of the 2nd and subsequent offences penalized by a maximum fine of WST100,000 (approx USD45,400) and/or 5 years imprisonment.
- International partnerships/limited partnerships: criminal offence punishable by a maximum fine of WST50,000 (approx USD22,700) and/or 5 years imprisonment.
- International trusts: criminal offence punishable by a maximum fine of WST50,000 (approx USD22,700) and/or 5 years imprisonment.

xv. Austria

Local laws should not apply if the reporting party has no Local Presence, and has not pass ported its license into Austria for purposes of the swap transactions. If there is activity or presence in Austria, the Austrian Data Protection Act 2000 applies to an entity (1) established in Austria; or (2) processing personal data is carried out in Austria or (3) in the case that the entity has no establishment in the EU, the reporting party uses processing equipment, e.g. a data center, located in Austria.

(a) Austrian Banking Act- banking secrecy obligation as stipulated in the Austrian Banking Act applies if:

- it is an Austrian credit institution (including investment management companies) licensed under the Austrian Banking Act;
- it is an Austrian branch of a non-EEA credit institution licensed under the Austrian Banking Act;
- it is a licensed EEA credit or financial institution (including investment management companies) or a licensed EEA investment firm that has pass ported its license into Austria in accordance with Section 9, 11 or 12 of the Austrian Banking Act or in accordance with Section 12 of the Austrian Securities Supervision Act; in this case, the licensed entity has to observe Section 38 Austrian Banking Act to the extent that it is conducting its services cross-border into Austria or through an Austrian branch.

Banking secrecy is not restricted to the licensed entity itself but also has to be observed by its shareholder(s), members of governing bodies, employees or by other persons/entities acting on behalf of such licensed entities (e.g. tax advisors, tied agents or third parties to which activities have been outsourced).

(b) Other Laws- Austrian Securities Supervision Act, the Austrian Payment Services Act and the Austrian E-Money Act contain secrecy obligations in relation to customer data. These provisions will apply to an entity that is established in Austria and that is:

- licensed as an investment firm (*Wertpapierfirma*) or an investment services provider (*Wertpapierdienstleistungsunternehmen*) in accordance with Section 3 or 4 of the Securities Supervision Act;
- licensed as a payment institution (*Zahlungsinstitut*) pursuant to the provisions of the Austrian Payment Services Act or
- licensed as an e-money institution (*E-Geld Institut*) pursuant to the provisions of the E-Money Act.

Secrecy obligations under these laws are not restricted to the licensed entity itself but also have to be observed by its employees or by other persons/entities acting on behalf of such licensed entities (e.g. tied agents or third parties to which activities have been outsourced).

The relevant regulations are:

- Austrian Data Protection Act 2000 (hereinafter "**DPA**"),
- Austrian Banking Act (hereinafter "**BWG**"), Section 38,
- Austrian Securities Supervision Act (hereinafter "**WAG**"), Section 7,
- Austrian Payment Services Act (hereinafter "**ZaDiG**"), Section 19 Para 4,
- Austrian E-Money Act (hereinafter "**E-GeldG**"), Section 13 Para 2.

For obtaining consent under the respective laws, the following has to be observed: The BWG requires that the entity bound by Section 38 BWG has to obtain the express and written consent of the customer to the disclosure of data protected by banking secrecy (Section 38 Para 2 Item 5 BWG). The WAG, the ZaDiG and the E-GeldG require that the entity bound the respective secrecy obligation needs to obtain written consent of the customer to the disclosure of the protected data.

- For consent to be sufficient, consent must b clear regarding the country to which the swap counterparty's personal data will be exported. Unless the receiving Swap Data Repository has obtained a certification under the Safe Harbor agreement (see http://safeharbor.export.gov/list.aspx) – the data export to the U.S. would require the prior approval of the Austrian Data Protection Commission which typically takes many months to obtain. An express consent language that would eliminate the prior approval requirement under the DPA would have to specifically refer to the fact that the receiving legal or regulatory authority or the trade repository are located in the United States. For obtaining consent under the BWG, the WAG, the ZaDiG or the E-GeldG, protocol consent language is not sufficiently clear. Consequently, there is the risk that this language will be unenforceable in Austria due to a lack of transparency. Language should explicitly state that the party whose data have

to be reported waives its right to secrecy under the BWG, the WAG, the ZaDiG or the E-GeldG, respectively, to the extent that parties have to meet reporting obligations to the SDR in accordance with the Dodd-Frank Act.

- Potential criminal and civil penalties for non-compliance-
    - Under the DPA, a data export without the prior approval of the Austrian Data Protection Commission (or the data subject's consent regarding the country in question) is subject to an administrative fine of up to EUR 10,000 (DPA § 52(2)(2)). This penalty would, in principle, be imposed on the members of management board of the reporting party entity in question, while the entity would be jointly and severally liable for any such fines (§ 9 of the Austrian Administrative Criminal Code).
    - Violations of Section 38 BWG (banking secrecy) constitute criminal offenses and are punishable with imprisonment of up to one year or a monetary fine of up to 360 daily rates. A daily rate is calculated on the basis of the personal and economical background of the offender at the time the judgment is passed. The judge may determine the daily rate in a range between EUR 4 and EUR 5,000 (Section 19 Austrian Penal Code). Further, the offender may become subject to damage claims.

Violations of Section 7 WAG, Section 19 Para 4 ZaDiG or Section 13 Para 2 E-GeldG constitute criminal offenses and are punishable with imprisonment of up to six months or a monetary fine of up to 360 daily rates. Further, the offender may become subject to damage claims.

xvi. Pakistan

Trade Participants may not be able to disclose any Trade Data about their respective counterparties unless (i) the prior written permission of the State Bank of Pakistan (the "**SBP**") has been obtained; or (ii) it is required by Pakistan law. The relevant provisions of Pakistan law include (a) Section 12 of the Banking Companies Ordinance, 1962 (the "BCO"); and (b) Section 33 of the BCO.

Accordingly, the use of an industry protocol to report Trade Data, or consent via a side letter, would not satisfy the statute's requirements. Disclosures made upon the request of foreign legal or regulatory authorities would similarly be in violation of local law. Potential liabilities for breaching Pakistan data privacy laws include damages, injunctive relief, action taken by the SBP (including cancellation of banking licence, penalties, removal of managerial personnel and prosecution of key officers) and criminal proceedings.

Certification Pursuant to Commission Regulation 140.99(c)(3)

As required by Commission Regulation 140.99(c)(3), I hereby (i) certify that the material facts set forth in the attached letter dated June 21, 2013 are true and complete to the best of my knowledge; and (ii) undertake to advise the Commission, prior to the issuance of a response thereto, if any material representation contained therein ceases to be true and complete.

Sincerely,

Robert Pickel