Juris Corp
advocates & solicitors

H. Jayesh
Talat Shah
Nisar Ookabhoy
* Fraser Mario Alexander
Huzefa Nasikwala
* Suruchi Dhavale
Freddy Daruwala
Sonali Sharma
Vandana Sekhri
Hoshedar Wadia

* Of Counsel

6th January 2010
JC/I-35-10/ 139 /2010
HHW/VSI/SDB

International Swaps and Derivatives Association, Inc.
24 Raffles Place
#22-00 Clifford Centre
Singapore 048621

Attn: **Mr. Keith Noyes**

Dear Sir,

Sub: **Legal validity of electronic transactions**

1) We refer to your email dated 21st October 2009. You have requested our advice on the enforceability of transactions under the ISDA Master Agreement which may be entered into by means of electronic data interchange or other means of electronic communication and the admissibility of electronic records in evidence in civil proceedings in India. You have sought our opinion on the following specific issues:

   (a) Does India have specific legislation giving legal recognition to electronic transactions and/or specific legislation dealing with the admissibility in evidence of electronic records? If there are no specific statutes, is it possible to justify the enforceability of electronic transactions and the admission into evidence of electronic records through legal reasoning? How robust would such a position be?

   (b) Would there be a presumption as to the authenticity and integrity of the electronic records?

   (c) What are the conditions (if any) that would need to be satisfied with regard to:
      (i) legal enforceability of electronic transactions;
      (ii) admissibility into evidence of electronic records; and
      (iii) presumption as to the authenticity and integrity of the electronic records?

   Though not relevant to the scope of this opinion (as the opinion primarily deals with evidentiary value of electronic records), it is pertinent to note that the Reserve Bank of India (**"RBI"**) as the banking regulator has imposed restrictions on the nature of transactions that can be entered into by 'Scheduled Commercial Banks'[1] through the internet as a mechanism or platform. These are set out, inter alia, in circulars issued by the RBI dated 14th June 2001[2] and 22nd August 2006[3] respectively. Relevant extracts of the circular are set out in Schedule I to this opinion. Although it is not clear from the circulars, we believe that the circulars are not intended to apply to inter-bank transactions.

[1] A bank included in Schedule II of the Reserve Bank of India Act, 1934. Practically every bank of material size including public sector and private sector Indian banks as well as Indian branches of foreign banks are included.
[2] DBOD.COMP.BC.130/ 07.03.23/ 2000-01
[3] DBOD No.Comp.BC.1658/07.23.29/2006-07

2) Assumptions
For the purpose of this opinion, we have made the following assumptions:
(a) The underlying transaction to be entered into by means of electronic data interchange or other means of electronic communication are valid and permitted under the laws of India; and
(b) One of the parties to the underlying transaction (referred to above) is a Scheduled Commercial Bank in India.

3) Before we address your specific queries the following background is relevant:
(a) The Information Technology Act, 2000 (the **"Infotech Act"**)
(i) The Infotech Act seeks to provide legal recognition for any transaction to be carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as **"Electronic Commerce"**. The Infotech Act was amended in 2008[4], inter alia, to provide recognition to alternate technology of electronic signatures[5] (**"Electronic Signature"**) in addition to Digital Signatures[6] (**"Digital Signature"**).
(ii) Section 2(1)(t) of the Infotech Act defines 'electronic record' as "data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche".
(iii) Section 4 of the Infotech Act provides that any information or other matters rendered or made available in an electronic form and accessible so as to be usable for a subsequent reference, will be legally recognised. Section 5 of the Infotech Act provides legal recognition of Electronic Signature as a substitute to handwritten signatures.
(iv) A Section 10-A has been introduced in the Infotech Act (which we believe is merely by way of clarification). Section 10-A of the Infotech Act provides that a contract formed by communication of proposals, revocation of proposals and acceptances, in electronic form, shall not be unenforceable merely because such contract has been formed using electronic means.
(v) Authentication
(A) Section 3 and 3-A of the Infotech Act respectively provide for authentication of electronic records by the use of Digital Signatures and Electronic Signatures.
(B) Under the Infotech Act, an electronic record is to be deemed as a 'secure electronic record' if the 'security procedure' has been applied to it (Section 14 of the Infotech Act). Similarly, an Electronic Signature shall be deemed to be a secure Electronic Signature, if the signature creation data, at the time of affixing such signature, was under the exclusive

[4] The Amendment Act came into force on 27th October, 2009.
[5] Section 2(1)(ta) of the Infotech Act defines Electronic Signature as 'authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature'. The contents of the Second Schedule are yet to be prescribed by the Central Government. Section 2(zg) read with Section 2(q) and Section 35(4) of the Infotech Act lays down that a subscriber is a person (which includes a corporate entity as well as an individual person) who has obtained a electronic signature certificate ("ESC") from a licensed certifying authority.
[6] According to Section 2(p) of Infotech Act, Digital Signature means 'authentication of an electronic record by a subscriber by means of electronic method or procedure in accordance with Section 3 of the Infotech Act'.

control of the signatory and the signature creation data was stored and affixed in such exclusive manner as may be prescribed by the Central Government (Section 15 of the Infotech Act). Section 2(1)(ze) read with Section 16 of the Infotech Act makes it necessary for the Central Government to prescribe the 'security procedure' to be applied to an electronic record to make it a 'secure electronic record'. Accordingly, under Indian laws, the authenticity and integrity of an electronic record or an Electronic Signature cannot be presumed unless it is a 'secure electronic record' or a secure Electronic Signature.

(C) Section 16 of the Infotech Act empowers the Central Government to prescribe security procedure for purposes of the Infotech Act. The Central Government has notified the Information Technology (Security Procedure) Rules, 2004 (**"Security Procedure Rules"**)[7]. According to Rule 3 of the Security Procedure Rules, a secure electronic record is one, which has been authenticated by means of a secure Digital Signature. Rule 4 of the Security Procedure Rules[8] lays down the procedure to be applied to a Digital Signature to make it a secure Digital Signature. Accordingly, if Digital Signature is being used, it has to comply with the requirements laid down under Rule 4 of the Security Procedure Rules. As stated above, it is pertinent to note that the Central Government has the authority to prescribe rules in relation to authentication of Electronic Signatures, but it is yet to prescribe the same.

(D) Section 12 of the Infotech Act relates to acknowledgement of receipt. Section 12 of the Infotech Act permits the originator to stipulate the manner in which the acknowledgment of having received an electronic record (i.e., instructions in this context) is to be issued. If the originator does not stipulate the manner of an acknowledgment, then such acknowledgment may be communicated in any form or implied by conduct. Section 12 of the Infotech Act also provides that if the person sending an electronic record stipulates that the same shall be binding only on receiving an acknowledgment from the other party that the other party has received the electronic record, then the same would be binding only upon receipt of such acknowledgement. Furthermore in such case, unless such acknowledgment has been received by the sender, it shall be deemed as if the electronic record was never sent.

(E) Section 13 of the Infotech Act contains provisions akin but not identical to the provisions of Indian Contract Act, 1872, relating to communication and acceptance of proposals. Section 13 of the Infotech Act states as follows:

> *"13. Time and place of despatch and receipt of electronic record*
>
> *(1) Save as otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters a computer resource outside the control of the originator.*

[7] Please note that these Security Procedures Rules currently apply only to Digital Signatures and not to Electronic Signatures. The provisions as regards Electronic Signatures have been enacted recently and the corresponding security procedures applicable to Electronic Signatures have not yet been issued.
[8] Please see Schedule II to this opinion, which contains an extract of Rule 4.

(2) *Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely: -*
   (a) *if the addressee has designated a computer resource for the purpose of receiving electronic records, -*
      (i) *receipt occurs at the time when the electronic record enters the designated computer resource; or*
      (ii) *if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;*
   (b) *if the addressee has not designated a computer resource alongwith specified timing, if any, receipt occurs when the electronic record enters the computer resource of the addressee.*

(3) ***Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be despatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.***

(4) *The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).*

(5) *For the purposes of this section, -*
   (a) *if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;*
   (b) *if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;*
   (c) *"usual place of residence", in relation to a body corporate, means the place where it is registered"* (emphasis supplied).

It is evident from the above that the parties are free to contract to the contrary.

We would also like to state that the 'computer resource' referred to above means any computer, computer system, computer network, data, computer database or software. For the purposes of this opinion, the designation of such resource can be generic (i.e. a particular trading platform).

(b) Indian Evidence Act, 1872 (the **"Evidence Act"**)

(i) The Infotech Act has made consequential amendments to the Evidence Act to include electronic records within the scope of evidence. Section 3 of the Evidence Act amends the definition of 'evidence' to include *"all documents including electronic records produced for the inspection of the Court"*. It is pertinent to note Section 19 of the Arbitration and Conciliation Act, 1996 which states that the arbitral tribunal shall not be bound by the Evidence Act. However, it does not mean that the arbitral tribunal ought not or should not consider and/or apply the principles of evidence. The arbitral tribunal, may not, consistent with the intent and object of the arbitration law, apply strict rules of evidence, but it is unlikely that it would disregard the rules of evidence which are founded on fundamental principles of justice and public policy. Therefore, the arbitral tribunal, would in our view, place reliance and give weightage to electronic form as a relevant and admissible form of evidence to decide the issue. However, the arbitral tribunal may well disregard the presumption and insist on having to prove it as against the onus on the other side having to disprove it.

(ii) Section 17 of the Evidence Act has been amended so as to include evidence contained in electronic format. Section 65A of the Evidence Act lays down that contents of electronic records may be proved according to provisions of Section 65B of the Evidence Act. According to Section 65B of the Evidence Act, an electronic record printed on paper or produced in magnetic or other media is a document and will be admissible as evidence without proof or production of original if:

[9]*"2. .....*

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

3. .....

4. In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,

[9] Section 65B of the Evidence Act, sub-section 2 onwards.

(a) identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate,

and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it."

(iii) Sections 85A and 85B of the Evidence Act provide for a presumption as to electronic agreement, electronic record and Electronic Signature. Section 85A of the Evidence Act stipulates that a court shall presume that every electronic record purporting to be an agreement containing the Electronic Signature of the parties was so concluded by affixing the Electronic Signature of the parties.

(iv) As per Section 85B of the Evidence Act, a court is required to presume in case of a secure electronic record that the same has not been altered since the specified point of time to which the secure status relates.

(v) As regards secure Electronic Signature, Section 85B of the Evidence Act stipulates that the court shall presume that the secure Electronic Signature was indeed affixed by the subscriber to whom it belongs and that too with the intention of signing or approving the electronic record.

Needless to add, the above presumptions can be sought to be rebutted by leading evidence to the contrary.

In other words, if the agreements have the secure Electronic Signature of the authorised user affixed to it, then the parties cannot seek to resile from the Electronic Transaction entered into on the grounds that the instruction was not communicated by the authorised user concerned.

(c) Stamp Duty

(i) In India, stamp duty is governed by Central (Government of India) legislation as well as State legislation. In the absence of a State legislation in a given State, the provisions of the Indian Stamp Act, 1899 (**"ISA"**) apply. The ISA has been amended to apply to various states by state level legislations extending to those states only. These state level legislations override the provisions of the ISA (except as regards certain instruments).

(ii) In our view, any transaction entered into by parties in electronic form, which would have attracted a stamp duty if it had been entered into in the physical/paper form, will also attract the same stamp duty (unless a different stamp duty has been prescribed). Certain state legislations, like the Bombay Stamp Act, 1958, and the Rajasthan Stamp Act, 1998 have been specifically amended to include electronic records. E-stamping is provided by the Stock Holding Corporation of India Limited and is currently available in certain states (Delhi, Gujarat, Karnataka, Maharashtra and Assam). Where e-stamping is

being used, we would advice the parties to independently evaluate the procedure stipulated before adopting the same. Where e-stamping is not available, the electronic confirmation will have to be printed out and stamped.

4) We shall now answer your queries in seriatim

(a) India has specific legislation that gives legal recognition to transactions entered into by means of electronic data interchange and other means of electronic communication, and also recognizes electronic documents as equivalent to physical documents. Please see our analysis in 3(a) above. India also has specific legislation which provides for an electronic record printed on paper or produced in magnetic or other media to be treated as a document and will be admissible as evidence. Please see our analysis in 3(b) above.

(b) Yes, there would be presumptions as to the authenticity and integrity of the **secure** electronic records (as distinct from just electronic record) and **secure** Electronic Signature (as distinct from just Electronic Signature). Please see our analysis in 3(a)(v)(B) and 3(b) above.

(c)

(i) Please see our response in 4(a) above.

(ii) Electronic records shall be deemed to be a document and shall be admissible in any proceedings, without further proof of production of the original, subject to the conditions mentioned in 3(b)(ii) above.

(iii) There would be presumptions as to authenticity and integrity of the **secure** electronic records and **secure** Electronic Signature. Section 85B of the Evidence Act lays down that the court shall presume that the **secure** electronic record has not been altered since the specific point of time to which the **secure** status relates. Similarly, when the **secure** Electronic Signature is affixed by the subscriber, the court shall presume that the Electronic Signature has been affixed with the intention of signing or approving the electronic record. Please see our analysis in 3(b)(iii), 3(b)(iv) and 3(b)(v) above. Currently, the Central Government has prescribed a security procedure in respect of secure Digital Signatures (which is one type of an Electronic Signature) only.

This opinion relates only to laws as applicable (including public policy) of the Republic of India as of the date hereof and as currently applied by Indian courts. This opinion is addressed to ISDA, solely for the benefit of its members. No other person may rely on this opinion for any purpose without our prior written consent. This opinion may, however, be shown by an ISDA member to a competent regulatory authority for such ISDA member, for the purposes of information only, on the basis that we assume no responsibility to such authority or any other person as a result, or otherwise.

Yours sincerely,

H Wadia.

Hoshedar Wadia
Juris Corp

Veena Sivaramakrishnan
Juris Corp

Schedule I

The following extract from RBI Circular dated 14th June 2001 on '*Internet Banking in India – Guidelines*' is relevant.

> *"As recommended by the Group, the existing regulatory framework over banks will be extended to Internet banking also. In this regard, it is advised that:*
>
> 1. *Only such banks which are licensed and supervised in India and have a physical presence in India will be permitted to offer Internet banking products to residents of India. Thus, both banks and virtual banks incorporated outside the country and having no physical presence in India will not, for the present, be permitted to offer Internet banking services to Indian residents.*
> 2. *The products should be restricted to account holders only and should not be offered in other jurisdictions.*
> 3. *The services should only include local currency products.*
> 4. *The 'in-out' scenario where customers in cross border jurisdictions are offered banking services by Indian banks (or branches of foreign banks in India) and the 'out-in' scenario where Indian residents are offered banking services by banks operating in cross-border jurisdictions are generally not permitted and this approach will apply to Internet banking also. The existing exceptions for limited purposes under FEMA i.e. where resident Indians have been permitted to continue to maintain their accounts with overseas banks etc., will, however, be permitted.*
> 5. *Overseas branches of Indian banks will be permitted to offer Internet banking services to their overseas customers subject to their satisfying, in addition to the host supervisor, the home supervisor."*

The aforementioned provisions were relaxed vide RBI Circular dated 22nd August 2006 on '*Internet Banking – Internet based platforms for dealing in foreign exchange*'. The following extract from the aforementioned circular is relevant.

> *"2. On a review it has been decided that banks may be permitted to offer Internet based foreign exchange services, for permitted underlying transactions, in addition to the local currency products already allowed to be offered on Internet based platforms, subject to the following terms and conditions:*
>
> *(i) Banks will remain responsible for secrecy, confidentiality and integrity of data.*
>
> *(ii) The data relating to Indian operations will be kept segregated.*
>
> *(iii) The data will be made available to RBI inspection / audit as and when called for.*
>
> *(iv) The services offered through Internet, for banks' customers on an Internet based platform for dealing in foreign exchange, should allow only reporting and initiation of foreign exchange related transactions, with the actual trade transactions being permitted only after verification of physical documents.*
>
> *(v) Banks should comply with FEMA regulations in respect of instructions involving cross-border transactions."*

Schedule II

"4. Secure digital signature

A digital signature shall be deemed to be a secure digital signature for the purposes of the Act if the following procedure has been applied to it, namely:-

(a) that the smart card or hardware token, as the case may be, with cryptographic module in it, is used to create the key pair;

(b) that the private key used to create the digital signature always remains in the smart card or hardware token as the case may be;

(c) that the hash of the content to be signed is taken from the host system to the smart card or hardware token and the private key is used to create the digital signature and the signed hash is returned to the host system;

(d) that the information contained in the smart card or hardware token, as the case may be, is solely under the control of the person who is purported to have created the digital signature;

(e) that the digital signature can be verified by using the public key listed in the Digital Signature Certificate issued to that person;

(f) that the standards referred to in rule 6 of the Information Technology (Certifying Authorities) Rules, 2000 have been complied with, in so far as they relate to the creation, storage and transmission of the digital signature; and

(g) that the digital signature is linked to the electronic record in such a manner that if the electronic record was altered the digital signature would be invalidated. "