

April 28, 2008

Mr. Rodney G. Vesling  
Senior Vice President and Officer, eTransactions  
Interlink Electronics, Inc.  
546 Flynn Road  
Camarillo, CA 93012

Re: Evaluation of Interlink's IntegriSign Emcee™ e-Signature Process Under the Electronic Signatures in Global and National Commerce Act ("ESIGN")

Dear Mr. Vesling:

Interlink has developed an online e-signature system called "IntegriSign Emcee™" (the "Emcee Solution") which may be used to create and execute one or more processes for presenting, signing, securing, archiving and retrieving electronic records relating to transactions in a variety of settings, including consumer transactions for financial services and products. (Each such process created by the Emcee Solution is referred to as the "Signing Ceremony"). Interlink has requested our<sup>1</sup> assessment of:

- whether transactions, including those related to financial services and products and transactions involving consumers, completed using the Emcee Solution are in accordance with the applicable electronic signature laws;
- the admissibility of the records presented, signed, secured, archived and retrieved by the Emcee Solution in an action to enforce the terms and conditions in such records signed using the Emcee Solution; and
- whether the terms and conditions in electronic documents signed using the Emcee Solution would be as enforceable against the signing party as would those same terms and conditions in paper documents signed in wet ink by that same person.

---

<sup>1</sup> The contributing authors of this letter are Greg Casamento and Patrick Hatfield. Greg practices in the area of electronic commerce and related litigation matters, including e-discovery and e-admissibility. Pat practices in the electronic commerce, intellectual property and technology areas. The conclusions herein are for informational purposes and are for the internal use of Interlink. The views expressed herein are those of the authors and do not constitute legal advice regarding any particular set of facts, products or services. The authors have not independently verified product or service features described herein and no endorsement is intended or implied. All descriptions of the features of the Emcee Solution are based on statements provided to us by Interlink, including those in Attachment 1 hereto, on which we have relied in expressing our views in this letter. The authors have given Interlink the right to reprint and distribute this paper, so long as it is reprinted in its entirety (including this notice), without alteration. ©2008 Locke Lord Bissell & Liddell LLP.

This letter discusses the statutory, regulatory and judicial authority existing as of the date hereof, but is not legal advice or a legal opinion as to a particular deployment of the Emcee Solution. We recommend that each company considering whether to deploy the Emcee Solution seek the advice of independent legal counsel with respect to how the topics discussed in this letter would apply to a particular deployment of the Emcee Solution.<sup>2</sup>

## **I. Executive Summary**

As noted above, Interlink has developed a process to complete transactions using electronic documents and electronic signatures. The Emcee Solution allows an Interlink client (a “User”) to configure the Emcee Solution to present electronic documents containing content otherwise compliant with applicable laws, such as consumer disclosure laws, and mandatory forms for the particular transaction in the sequence required by law. Users may configure the Emcee Solution to present one or more electronic documents to each person who is to sign each such document using an electronic signature (a “Signer”). The Signer would have the ability to view in its entirety each document he or she is prompted to sign. Upon signing of each such electronic document by a Signer, the Emcee Solution secures that document in a way that would reveal whether that document has been altered after it was signed by that Signer. The Emcee Solution also allows Users to archive each record securely in a way that would reveal whether the signed document was altered after it was signed, archived and retrieved.

For the reasons explained below, for a User who uses the Emcee Solution to create Signing Ceremonies to present documents containing content otherwise enforceable and compliant with applicable laws, such as consumer disclosure laws, and mandatory forms for the particular transaction, it is our view that:

- The Emcee Solution would allow the User to present transaction documents to be executed by the relevant parties to such documents, in such a way that the execution of such documents would be in accordance with the applicable electronic signature laws;
- The electronic documents presented, signed, secured, archived and retrieved using such Signing Ceremonies created using the Emcee Solutions would be as enforceable against the Signer as would a wet ink signature by that same person on hard copies of such documents containing those same terms and conditions; and
- Such electronic documents presented, signed, secured, archived and retrieved using such Signing Ceremonies created using the Emcee Solution would, assuming the proponent lays the appropriate foundation, be as admissible in a

---

<sup>2</sup> Subject to applicable rules governing our professional responsibilities, companies considering deploying the Emcee Solution who would like our advice on a particular deployment of the Emcee Solution may contact us directly. We may be able to advise on the enforceability of certain transactions using the Emcee Solution in a specific deployment of the Emcee Solution more efficiently than others because of our familiarity with the Emcee Solution.

court of law in an action to enforce such terms and conditions as would such documents presented, signed, archived and retrieved in wet ink and paper.

## **II. Background and Scope**

Attached to this letter is a Glossary of Terms describing capitalized terms used below, as well as two Attachments. Attachment 1 hereto contains a number of statements which you have told us accurately describe the Emcee Solution. For purposes of our views in this letter, we have assumed each of those statements to be accurate, as the Emcee System is configured by a User for a particular deployment. Attachment 2 contains descriptions you have provided to us, which we also assume to be accurate, as to *how* the Emcee Solution satisfies the statements contained in Attachment 1 hereto.

We are also assuming in this letter that the types of transactions to be created by Users and completed by Signers of the Emcee Solution are not in any of the following areas:

- transactions dealing with the specific areas of the law expressly excluded from the federal ESIGN law, as described immediately below;
- transactions dealing with any governmental agency where that agency is acting as a market participant; or
- execution of documents required by any governmental agencies which are not related to transactions between private parties, even if those documents are permitted to be filed with such agency exclusively through electronic means, such as documents required to be filed with or maintained for inspection by the SEC or FDA.<sup>3</sup>

ESIGN does not apply to contracts and records that are governed by laws and regulations in the following areas:

- wills, codicils, and testamentary trusts;
- a State statute, regulation, or other rule of law governing adoption, divorce, or other matters of family law;
- the Uniform Commercial Code, as in effect in any State, other than sections 1-107 and 1-206 and Articles 2 and 2A;
- court orders or notices, or official court documents required to be executed in connection with court proceedings;

---

<sup>3</sup> This is not to say that the Emcee Solution is not configurable to meet the requirements of a governmental agency's requirements for executing documents not relating to transactions. Rather, this assumption is simply to alert the reader that certain governmental agencies may take the position that documents not related to transactions between private parties may not be within the scope of ESIGN and UETA.

- notices for cancellation or termination of utility services (including water, heat, and power);
- notices of default, acceleration, repossession, foreclosure, or eviction, or the right to cure, under a credit agreement secured by, or a rental agreement for, a primary residence of an individual;
- notices of cancellation or termination of health insurance or benefits or life insurance benefits;
- recall notices of a product, or material failure of a product that risks endangering health or safety; and
- any document required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic and dangerous materials.<sup>4</sup>

Notwithstanding the foregoing exceptions, ESIGN (and UETA), when applied with other laws such as Revised Article 9 of the Uniform Commercial Code, provide a mechanism for the use of electronic signatures and records in many of the most common business and consumer transactions, including generally, without limitation, contracts and records involving: (i) sales and leases of goods; (ii) insurance applications; (iii) mortgage loan documentation; and (iv) banking and investment transactions. For example, while it is beyond the scope of this letter to examine how the Emcee Solution might generate the appropriate records for electronic chattel paper under Revised Article 9, we believe that the Emcee Solution is capable of being configured to generate documents satisfying the requirements of electronic chattel paper under Revised Article 9.

ESIGN, the federal law, specifically applies to the business of insurance.<sup>5</sup> Given the similarity between ESIGN and UETA, insurance companies and other firms regulated under the insurance codes of the states, can adopt a uniform, national e-sign process.

### **III. Legal Analysis**

#### **A. ESIGN vs. UETA**

For all purposes relevant to the analysis in this letter, except as noted otherwise, the analysis under ESIGN (the federal statute) and the relevant enacted version of UETA, which all but four (4) states have adopted, are essentially the same.<sup>6</sup> For those states that have adopted electronic signature laws governing interstate commerce inconsistent with ESIGN in areas relevant to the issues discussed in this letter, such state laws will be preempted by ESIGN's

---

<sup>4</sup> ESIGN § 7003 (a),(b).

<sup>5</sup> ESIGN § 101(i).

<sup>6</sup> The states that have not adopted UETA are Georgia (adopted Electronic Records and Signatures Act), Illinois (adopted Electronic Commerce Security Act), New York (adopted Electronic Signatures and Records Act), and Washington (adopted Electronic Authentication Act).

broad preemption provisions.<sup>7</sup> For those states that have not adopted any electronic signature laws, ESIGN will govern as a result of its broad preemption provisions.<sup>8</sup>

B. General - Electronic Signatures May Not Be Denied Legal Effect

ESIGN recognizes that an electronic signature may be as legally effective as a signature applied in wet ink on paper. ESIGN does not give electronic signatures a special status in the law. Rather, ESIGN states that a signature may not be denied legal effect *solely* because it is in electronic form. The foundational provision of ESIGN acknowledging electronic signatures provides:

(a) In General.--Notwithstanding any statute, regulation, or other rule of law (other than this title and title II), with respect to any transaction in or affecting interstate or foreign commerce--

(1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and

(2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.<sup>9</sup>

ESIGN, as does UETA,<sup>10</sup> gives equal recognition to electronic signatures, with the few exceptions mentioned above and which are not relevant here.

C. “Electronic Signature” Defined

If a signature is created using a “sound, symbol or process” that is “attached to or logically associated with” a contract or other record by a person intending to sign such contract or record, such signature will be legally effective. For ease of reading this letter, phrases such as “legally effective” are used, rather than the more technically correct phrase, “not be denied legal effect solely because such signature is an electronic signature.” ESIGN defines an “electronic signature” as:

(5) Electronic signature.--The term “electronic signature” means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.<sup>11</sup>

ESIGN defines “electronic record” as:

---

<sup>7</sup> ESIGN § 102(a).

<sup>8</sup> ESIGN § 102(a).

<sup>9</sup> ESIGN § 101(a).

<sup>10</sup> UETA § 7(a).

<sup>11</sup> ESIGN § 106(5).

(4) Electronic record.--The term "electronic record" means a contract or other record created, generated, sent, communicated, received, or stored by electronic means.<sup>12</sup>

ESIGN defines "record" as:

(9) Record.--The term "record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.<sup>13</sup>

Thus, an electronic signature may consist of an electronic sound or symbol, such as an individual saying "I agree," typing "I agree" or the person's name or following some other process, such as clicking "I agree," which is attached to or logically associated with information inscribed: (i) on a tangible medium, such as the tangible, hard copy of an authorization; or (ii) stored in an electronic medium retrievable in a perceivable form, such as the electronic record containing the identical information as contained in the tangible hard copy delivered to the consumer. The Emcee Solution allows the User to select from a variety of methods of generating the Signer's actual signature. In any event, the User has the ability to configure the Emcee Solution to use an electronic sound, symbol, or process which is then attached to or logically associated with particular terms and conditions in a record, where it is clear to the Signer that using such electronic sound, symbol, or process is how the Signer expresses his or her consent to sign such document containing particular terms and conditions.

Evidence of the person's intent to sign the record (which would be required if the person signed in ink on a piece of paper) may be inferred (as it is from ink on paper) from words close to the place of the signature where such words indicate in clear and conspicuous terms the person's intent to sign and be bound thereby. For example, the text in the ESIGN Consent could include the following text to explain the legal significance of the Signer using the Emcee Solution to create his or her electronic signature: "By [describe method used to consent, e.g., selecting "I AGREE"], you confirm that you have the computer hardware and software to access electronic records in the form that important disclosures will be provided to you in connection with [describe transactions], and you consent to receiving consumer disclosures related to [describe transaction] exclusively through electronic means."

Accordingly, pursuant to ESIGN and UETA, the electronic signature created by the Emcee Solution should not be denied legal effect solely because it is in electronic form. Similarly, a document relating to such transaction should not be denied legal effect, validity or enforceability solely because the electronic signature used to sign such document was used in its formation and stored as an electronic record, rather than in hard copy.

#### D. Consumer Disclosures

---

<sup>12</sup> ESIGN § 106(4).

<sup>13</sup> ESIGN § 106(9).

ESIGN provides that, upon consent by the consumer, certain information relating to a transaction or transactions in or affecting interstate or foreign commerce, which is required by a statute, regulation, or rule of law (other than E-SIGN) to be provided or made available to a consumer in writing (a "Special Consumer Disclosure") may be delivered exclusively via electronic means, provided, that the recipient of the Special Consumer Disclosure is first provided, and agrees to, the E-SIGN Consent.<sup>14</sup> Whether a particular transaction requires a Special Consumer Disclosure, and the how the E-SIGN Consent is provided in connection with the required Special Consumer Disclosure, must be determined on a transaction-by-transaction basis. The Emcee Solution allows the User to identify which documents are Special Consumer Disclosures triggering the need for the E-SIGN Consent in the context of each type of transaction completed using the Emcee Solution. The E-SIGN provisions describing what is a "Special Consumer Disclosure" and the contents of the E-SIGN Consent are recited below:

If a statute, regulation, or other rule of law requires that information relating to a transaction or transactions in or affecting interstate or foreign commerce be provided or made available to a consumer *in writing*, the use of an electronic record to provide or make available (whichever is required) such information satisfies the requirement that such information be in writing if--

(A) the consumer has affirmatively consented to such use and has not withdrawn such consent;

(B) the consumer, prior to consenting, is provided with a clear and conspicuous statement--

(i) informing the consumer of (I) any right or option of the consumer to have the record provided or made available on paper or in nonelectronic form, and (II) the right of the consumer to withdraw the consent to have the record provided or made available in an electronic form and of any conditions, consequences (which may include termination of the parties' relationship), or fees in the event of such withdrawal;

(ii) informing the consumer of whether the consent applies (I) only to the particular transaction which gave rise to the obligation to provide the record, or (II) to identified categories of records that may be provided or made available during the course of the parties' relationship;

(iii) describing the procedures the consumer must use to withdraw consent as provided in clause (i) and to update information needed to contact the consumer electronically; and

---

<sup>14</sup> E-SIGN §7001(c).

(iv) informing the consumer (I) how, after the consent, the consumer may, upon request, obtain a paper copy of an electronic record, and (II) whether any fee will be charged for such copy;

(C) the consumer--

(i) prior to consenting, is provided with a statement of the hardware and software requirements for access to and retention of the electronic records; and

(ii) consents electronically, or confirms his or her consent electronically, in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent; and

(D) after the consent of a consumer in accordance with subparagraph (A), if a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the consumer will not be able to access or retain a subsequent electronic record that was the subject of the consent, the person providing the electronic record--

(i) provides the consumer with a statement of (I) the revised hardware and software requirements for access to and retention of the electronic records, and (II) the right to withdraw consent without the imposition of any fees for such withdrawal and without the imposition of any condition or consequence that was not disclosed under subparagraph (B)(i); and

(ii) again complies with subparagraph (C).

The Signer's affirmative consent to the E-SIGN Consent must exhibit the Signer's ability to access information in the manner that the Special Consumer Disclosures will be provided. For example, if the required disclosure (a truth in lending notice for example) will be posted at a secure web site accessible only after the Signer is given a unique access code, the Signer should be given that unique access code during the E-SIGN Consent process to confirm that the unique access code in fact allowed the Signer to access the secure site where Special Consumer Disclosures, such as the truth in lending statement, will be posted.

If the Signer consents to receive disclosures electronically but does not reasonably demonstrate his or her ability to access information in the manner the Special Consumer Disclosures are provided, then the Special Consumer Disclosure is likely to be ineffective and therefore the basis for providing the required disclosures exclusively by electronic means could fail. Failure to comply with the E-SIGN consumer disclosure requirements does not, however, render void or voidable the underlying transaction. E-SIGN provides:

(3) Effect of failure to obtain electronic consent or confirmation of consent.--The legal effectiveness, validity, or enforceability of any contract executed by a consumer shall not be denied solely because of the failure to obtain electronic consent or confirmation of consent by that consumer in accordance with paragraph (1)(C)(ii).<sup>15</sup>

Failure to comply with the ESIGN consumer disclosure requirements could, however, subject the User to regulatory sanctions for failing to provide the required disclosures (such as the truth in lending notice in the example above) in accordance with applicable law. There may also be civil remedies available to Signers if the disclosures are deemed to have not been given effectively.

Not all notices or documents Users are required to provide to Signers are Special Consumer Disclosures subject to the ESIGN disclosure requirements above. For such notices and documents which are *not* such “Special Consumer Disclosures,” the Signer only needs to agree to receive such notices and documents exclusively via electronic means.

The Emcee solution allows the User to designate which records are Special Consumer Disclosures and, where there are Special Consumer Disclosures for a particular transaction, the User may configure the Emcee Solution to: (1) present the appropriate ESIGN Consent to the Signer, (2) record whether the Signer consented to receive Special Consumer Disclosures exclusively through electronic means in a way that reasonably demonstrates the ability of the Signer to access information in the electronic format the actual Special Consumer Disclosure will be provided or made available to the Signer, and (3) for the Special Consumer Disclosures to then provide or make available to the Signer such disclosures in that same format. As such, the User may configure the Emcee Solution to provide Special Consumer Disclosures in accordance with the requirements of ESIGN.

Interestingly, use of an electronic process to complete transactions requiring Special Consumer Disclosures, or other documents containing mandated terms such as pre-approved forms, can actually reduce the User’s compliance risk, compared to conventional approach of paper and ink. The Emcee Solution allows Users to specify each document that must be presented and signed, as an acknowledgment of receipt or otherwise, as a condition to completing the transaction. Further, Users may configure the Emcee Solution to specify which fields must be completed (as well as the nature of the information completed in such field, such as ineligible states. Such configurability allows Users to specify each step to be completed as a condition to complete the transaction. Stated otherwise, Users may configure the Emcee Solution to prevent incomplete or non-compliant transactions from being submitted to the User for review. This can significantly improve a User’s ability to comply with the requirements for such regulated transactions, reduce risk while at the same time improve the rate of successfully completed transactions.

#### E. Verifications and Acknowledgements

---

<sup>15</sup> ESIGN § 101(c)(3).

Verifications and acknowledgments required by law are expressly permitted to be delivered in electronic form under ESIGN in certain circumstances. ESIGN provides:

(B) Verification or acknowledgment.--If a law that was enacted prior to this Act expressly requires a record to be provided or made available by a specified method that requires verification or acknowledgment of receipt, the record may be provided or made available electronically only if the method used provides verification or acknowledgment of receipt (whichever is required).<sup>16</sup>

Thus, if a law requires a disclosure to be provided by a certain method, which requires acknowledgment of receipt, such as delivery by first class mail, with proof of delivery required, such verification or acknowledgment may be given electronically if, and only if, the electronic method for providing such verification or acknowledgment also provides verification or acknowledgment of receipt. For example, the Emcee Solution can be configured so that the consumer, prior to reviewing the verification or acknowledgement, is asked to confirm receipt.

#### F. Record Retention- Electronic Records Can be Sufficient

There are two (2) record retention issues addressed by ESIGN. The first relates to the requirement that, where a statute requires a contract or other document to be in writing, the electronic record of such contract or document may be denied legal effect if the electronic record cannot be reproduced for reference by all parties or persons entitled to the contract. The relevant section of ESIGN provides:

(e) Accuracy and Ability To Retain Contracts and Other Records.--Notwithstanding subsection (a), if a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be in writing, the legal effect, validity, or enforceability of an electronic record of such contract or other record may be denied if such electronic record is not in a form that is capable of being retained and accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record.<sup>17</sup>

Thus, if a User is going to rely exclusively on the archived electronic record to satisfy the statutory requirement that a contract or other document be in writing, failure to maintain the record in a form capable of being retrieved by all parties for later reference, could jeopardize the enforceability of the transaction to which such record relates. The Emcee Solution allows Users to satisfy this requirement by making the electronic record available to the Signer for the required period of time or the User can send a copy of the document(s), in hard copy or otherwise so the User is not relying on the Signer's ability to access the electronic record maintained by the User.

---

<sup>16</sup> ESIGN § 101(c)(2)(B).

<sup>17</sup> ESIGN § 101(e).

In contrast, the second record retention issue relates to the User satisfying statutory record retention obligations. The User may store electronically the record (whether that record was initially in tangible form and later converted to an electronic form or initially in electronic form) of a transaction and thereby satisfy the statutory record retention requirement, provided certain conditions are met. The relevant portion of ESIGN provides:

(d) Retention of Contracts and Records.--

(1) Accuracy and accessibility.--If a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be retained, that requirement is met by retaining an electronic record of the information in the contract or other record that--

(A) accurately reflects the information set forth in the contract or other record; and

(B) remains accessible to all persons who are entitled to access by statute, regulation, or rule of law, for the period required by such statute, regulation, or rule of law, in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise.

(2) Exception.--A requirement to retain a contract or other record in accordance with paragraph (1) does not apply to any information whose sole purpose is to enable the contract or other record to be sent, communicated, or received.

(3) Originals.--If a statute, regulation, or other rule of law requires a contract or other record relating to a transaction in or affecting interstate or foreign commerce to be provided, available, or retained in its original form, or provides consequences if the contract or other record is not provided, available, or retained in its original form, that statute, regulation, or rule of law is satisfied by an electronic record that complies with paragraph (1).<sup>18</sup>

ESIGN permits Users to satisfy their record retention obligations relating to transactions by retaining documents exclusively through electronic means. These ESIGN record retention requirements do not affect Users' record retention practices, except for those records relating to transactions to be retained exclusively through electronic means. Thus, if the User is satisfying the record retention obligations imposed on it by other laws by storing hard copies, ESIGN will not impose additional obligations.

As noted above, ESIGN does permit companies to satisfy the record retention requirements imposed by statute by retaining only the electronic records, if the requirements of

---

<sup>18</sup> ESIGN § 101(d).

Section 101(e) of E-SIGN are met. Thus, if documents in the Audit Trail, which are required by law to be retained, are retained exclusively in electronic media, and are available to the regulators having jurisdiction over the Company and such electronic records are available in accordance with Section 101(e) of E-SIGN, the User may not be required to print and retain hard copies of these documents.

#### G. Risk Analysis Framework

Discussed below are certain risks presented with any transaction, not just electronic transactions. Users have the ability to configure the Emcee Solution by defining the rules for each type of Signing Ceremony to address these risks which we believe are material to designing and implementing an effective, enforceable electronic contracting process.

##### ***Authentication Risk***

This is the risk that a party electronically signing a document is in fact not the person he or she claims to be. Users may configure the Emcee Solution to authenticate the identity of each Signer in a variety of ways. The method chosen by the User to authenticate a given Signer is included in the archived signing session, or Audit Trail, which is then securely archived and capable of being retrieved securely. The authentication, or forgery, risk is also present for documents signed in paper and wet ink. Users can configure the Emcee Solution to calibrate the level of authentication with their own assessment of the authentication risk.

##### ***Repudiation Risk***

This is the risk of a Signer acknowledging that he or she signed a document, but claiming that the electronic signature is attached to or logically associated with a document containing terms and conditions different than or possibly in addition to those in the document the Signer signed. The risk is that the Signer repudiates the terms and conditions in the document attached to or logically associated with his or her signature and thereby reduces the chance that such document will be admissible into evidence and, if admitted into evidence, that the tier of fact will be persuaded that the Signer in fact agreed to be bound by all such terms and conditions.

The Emcee Solution contains features that can reduce the repudiation risk far below the repudiation risk associated with paper documents and wet ink. Users may configure the Emcee Solution to cryptographically seal each document upon execution of that document by each Signer, thereby rendering such document unalterable without detection. Documents electronically sealed in this fashion are likely to pass the admissibility threshold (see discussion below) and once such documents are admitted into evidence, Users are likely to have meaningful, persuasive evidence as to why such document could not have been alerted without detection.

##### ***Admissibility Risk***

This is the risk that a court refuses to admit into evidence copies of electronic documents generated, presented, signed, secured, archived and retrieved by the Emcee Solution.

Preliminarily, it is important to recognize that all of the rules of evidence and evidentiary foundations that apply to paper documents and wet ink signatures apply also to electronic documents signed electronically, stored electronically and retrieved electronically. The Federal Rules of Evidence, or their state equivalents, govern the admissibility of evidence and thus would govern the admissibility of a copy of a document presented, signed, secured, archived and retrieved by the Emcee Solution.<sup>19</sup>

Users may use the Emcee Solution create Signing Ceremonies to satisfy the admissibility standards in the Federal Rules of Evidence to prove at trial the authenticity of a document retrieved by the Emcee Solution because the Signing Ceremonies can create a record of the entire signature ceremony process, including: (a) the terms and conditions presented to the Signer with which the electronic signature will be logically associated; (b) the specific act of the Signer expressing his or her intent to be bound to those terms and conditions, as called for in those same terms and conditions; and (c) the circumstances under which signatures were obtained. This information all goes to establish the authenticity of the document (containing the terms and conditions) retrieved by the Emcee Solution. The Emcee Solution allows Users to securely archive and retrieve the documents in a way to show that the documents containing the signatures could not have been altered without detection. Users may configure the Emcee Solution to enable the appropriate witness from Interlink or the User to provide an affidavit or live testimony as to the foregoing. For the reasons described below, such copies of documents generated by the Emcee Solution based on documents presented, signed, secured, archived and retrieved by the Emcee Solution should be as admissible under the Federal Rules of Evidence as such documents containing the same terms and conditions generated, presented, signed in hard copy and wet ink, where such paper copy is secured, archived and retrieved using conventional archival and retrieval methods.<sup>20</sup>

The standard for the authentication of evidence under the Federal Rules of Evidence is contained in Rule 901, Requirement of Authentication or Identification, which provides that “the requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.”<sup>21</sup> As stated throughout the case law involving computer generated information “‘reliability must be the watchword’ in determining the admissibility of computer generated evidence.”<sup>22</sup> The “factors [must] effectively address a witness’ familiarity with the type of evidence and the method used to create it, and appropriately require that the witness be

---

<sup>19</sup> Many states have adopted rules of evidence that track the Federal Rules of Evidence (FRE). For purposes of this discussion all cited cases are based on the FRE or state law that follows the FRE.

<sup>20</sup> This would require the User to identify who, by name and title, is qualified to testify (in person or via affidavit) as to how each document was presented, signed, secured after signature to render it unalterable without detection, archived, retrieved and printed. This person will also testify as to the integrity and security of each system involved in creating, securing, archiving, retrieving and printing the document.

<sup>21</sup> See also *Lorraine v. Markel American Insurance Company*, 241 F.R.D. 534, 541-42 (D.Md. 2007).

<sup>22</sup> *State v. Swinton*, 268 Conn. 781, 812 (CT. 2004) (applying the federal standard to a state case.)

acquainted with the technology involved in the computer program used to generate the evidence.”<sup>23</sup>

Certain subparts of Sections 901 and 902 of the Federal Rules of Evidence are particularly suited to address the admission of electronic signatures and records: Sections 901(b)(1), (3), (4) and (9), and 902(7) and (11). Rules 901(b)(1), (3), (4) and (9) require witness testimony to authenticate proffered evidence, while 902(7) and (11) allow for self-authentication.<sup>24</sup>

### ***F.R.E. 901***

A witness with direct knowledge, pursuant to F.R.E. 901(b)(1), or an expert witness with learned knowledge, pursuant to F.R.E. 901(b)(3), are certainly two fairly straightforward methods a User could use to admit hard copies of documents signed using the Emcee Solution. F.R.E. 901(b)(4), which permits exhibits to be authenticated by appearance, contents, substance, internal patterns, or other distinctive characteristics “is one of the most frequently used [rules] to authenticate [electronic signatures] and other electronic records.”<sup>25</sup> F.R.E. 901(b)(9), which authorizes authentication by “[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result”, is “one method of authentication that is particularly useful in authenticating electronic evidence stored in or generated by computers” and is frequently used as a litmus test for admissibility of computer-related information.<sup>26</sup> “[It] dictates that the inquiry into the basic foundational admissibility requires sufficient evidence to authenticate both the accuracy of the image *and* the reliability of the machine producing the image.”<sup>27</sup>

The process used by the Emcee Solution to secure each document after it is signed allows Users to configure the Emcee Solution to meet the admissibility standards under the subsections in F.R.E. 901. The testimony of a witness with knowledge of the specific transaction will satisfy F.R.E. 901(b)(1), and a learned expert witness should suffice under F.R.E. 901(b)(3). A witness

---

<sup>23</sup> *Id.* at 813, 814.

<sup>24</sup> Magistrate Judge Paul W. Grimm’s opinion in *Lorraine v. Markel American Insurance Company* provides one of the best analysis to date of the admissibility of electronic evidence, which broadly could include electronic signatures. 241 F.R.D. at 542. See, e.g.: *In Re Vee Vinhnee*, 336 B.R. 437 (proponent failed properly to authenticate exhibits of electronically stored business records); *United States v. Jackson*, 208 F.3d 633, 638 (7th Cir. 2000) (proponent failed to authenticate exhibits taken from an organization’s website); *St. Luke’s Cataract and Laser Institute PA v. Sanderson*, 2006 WL 1320242, at \*3-4 (M.D. Fla. May 12, 2006) (excluding exhibits because affidavits used to authenticate exhibits showing content of web pages were factually inaccurate and affiants lacked personal knowledge of facts); *Rambus v. Infineon Tech. A.G.*, 348 F. Supp. 2d 698 (E.D. Va. 2004) (proponent failed to authenticate computer generated business records); *Wady v. Provident Life and Accident Ins. Co. of Am.*, 216 F. Supp. 2d 1060 (C.D. Cal. 2002) (sustaining an objection to affidavit of witness offered to authenticate exhibit that contained documents taken from defendant’s website because affiant lacked personal knowledge); *Indianapolis Minority Contractors Assoc. Inc. v. Wiley*, 1998 WL 1988826, at \*7 (S.D. Ind. May 13, 1998) (proponent of computer records failed to show that they were from a system capable of producing reliable and accurate results, and therefore, failed to authenticate them).”

<sup>25</sup> *Lorraine* at 544.

<sup>26</sup> *Id.* at 549.

<sup>27</sup> *Swinton*, 268 Conn. at 811.

knowledgeable about the contents, substance and distinctive characteristics of the Emcee Solution and the process of creating, presenting, signing, securing, archiving and retrieving the documents in question should satisfy F.R.E. 901(b)(4), while testimony describing how the Emcee Solution accomplishes the foregoing accurately should suffice under F.R.E. 901(b)(9).

In addition to the express language of F.R.E. 901(b)(9), Imwinkelried's *Evidentiary Foundations* provides a supplemental eleven-step process under the Rule for the admission of computer generated records.<sup>28</sup> Most of the testimony proffered under these eleven steps is a simple recitation of facts that the Emcee Solution should meet. More challenging is step four, which requires proof that the "procedure has built-in safeguards to ensure accuracy and identify errors...regarding computer policy and system control procedures, including control of access to the database, control of access to the program, recording and logging changes, backup practices, and audit procedures to assure the continuing integrity of the records."<sup>29</sup> In satisfying this requirement or making arguments for admissibility under 901(b)(4), the User would need to provide expert technical testimony as to the functionality and safeguards in the Emcee Solution deployed by that User.

Witness testimony seeking the admission of signatures and documents from the Emcee Solution pursuant to F.R.E. 901(b)(9) would include:

- The manner in which the User's or Emcee Solution's server(s), as appropriate, are used to generate electronic signatures and documents;
- The reliability of these servers;
- Procedures for manual data entry and system controls; and
- Safeguards to ensure accuracy and identify errors (i.e., safeguards, access rules and other controls on the environment that govern the flow of information through

---

<sup>28</sup> Edward J. Imwinkelried, *Evidentiary Foundations*, 58-59 (LexisNexis 6th ed. 2005).

1. The business uses a computer.
2. The computer is reliable.
3. The business has developed a procedure for inserting data into the computer.
4. The procedure has built-in safeguards to ensure accuracy and identify errors.
5. The business keeps the computer in a good state of repair.
6. The witness had the computer readout certain data.
7. The witness used the proper procedures to obtain the readout.
8. The computer was in working order at the time the witness obtained the readout.
9. The witness recognizes the exhibit as the readout.
10. The witness explains how he or she recognizes the readout.
11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.

<sup>29</sup> *In re Vee Vinhnee* at 447. Opposing parties often allege that computer records have been tampered with and thus lack authenticity. Such claims have been viewed as "almost wild-eyed speculation...without some evidence to support such a scenario..." *United States v. Whitaker*, 127 F.3d 595, 602 (7th Cir. 1997).

its system), tamper resistant software, use of cryptographic technology, and that all of these meet or exceed industry standards.

Following initial court decisions recognizing the safeguards of a particular Emcee Solution, parties may stipulate to the authenticity of electronic signatures created by that and comparable Emcee Solutions, so that in the initial cases witness testimony is required but in future and subsequent cases it is not. Notwithstanding, at the present time there is ample evidence to lay the appropriate foundation for the admission of electronic signatures created by using the Emcee Solution.

### ***F.R.E. 902***

Although in a major dispute testimony may be necessary regarding the Emcee Solution and the authenticity of its process, as noted above, documents presented, signed, secured, archived and retrieved using the Emcee solution may also be admitted as self-authenticating documents under F.R.E. 902(7). Judge Grimm in the extremely thorough opinion in *Lorraine v. Markel*, stated that: “[e]xtrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to the following:...(7) Trade inscriptions and the like. Inscriptions, signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin.”<sup>30</sup> “Under Rule 902(7), labels or tags affixed in the course of business require no authentication. The Emcee Solution will collect and record information showing the entire signature ceremony. The identification markers alone stored in the secure container may be sufficient to authenticate an *electronic record* and *electronic signature* under Rule 902(7).”<sup>31</sup>

F.R.E. 902(11) of the Federal Rules of Evidence is the other subsection that might be considered for authentication of documents presented, signed, secured, archived and retrieved using the Emcee Solution’s electronic signatures. As Judge Grimm noted: “Rule 902(11) also is extremely useful because it affords a means of authenticating business records under Rule 803(6), one of the most used hearsay exceptions, without the need for a witness to testify in person at trial.”<sup>32</sup> The primary reason one would seek to authenticate ESI using this rule is that it permits a written declaration by a custodian rather than oral testimony, which under most circumstances makes it preferable to F.R.E. 901(b)(4) or (b)(9). F.R.E. 902(11) addresses:

Certified domestic records of regularly conducted activity. The original or a duplicate of a domestic record of regularly conducted activity that would be admissible under Rule 803(6) if accompanied by a written declaration of its custodian or other qualified person, in a manner complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority, certifying that the record-

---

<sup>30</sup> *Lorraine* at 549.

<sup>31</sup> *Id.*, quoting *Weinstein’s Federal Evidence* § 900.07[3].

<sup>32</sup> *Lorraine* at 552.

- (A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;
- (B) was kept in the course of the regularly conducted activity; and
- (C) was made by the regularly conducted activity as a regular practice.<sup>33</sup>

“Rule 902(11) was designed to work in tandem with an amendment to Rule 803(6) to allow proponents of business records to qualify them for admittance with an affidavit or similar written statement rather than the live testimony of a qualified witness. In addition to the affidavit requirements, there is a notice requirement to afford opposing parties an opportunity to review the document and affidavit to challenge its authenticity.<sup>34</sup> Thus, assuming no challenge, F.R.E. 902(11) is one of the best ways to secure the admission of signatures and documents executed using the Emcee Solution.

As explained above, critical in the admissibility analysis and the overall enforceability of documents executed using the Emcee Solution is the requirement of a secure method to archive and retrieve the documents. We understand that Interlink has relationships with third parties to provide such “e-vaulting” secure archival and retrieval service to be used with the Emcee Solution.

### ***Compliance Risk***

Users may configure the Emcee Solution to meet the following regulatory requirements:

- Assure that each document presented and/or signed by a Signer complies with the legal requirements for the content, presentation, sequence and information to be obtained for each such document;
- For Special Consumer Disclosures, the Signer is provided the appropriate information to then make the informed consent in a way that complies with the consumer disclosure requirements of ESIGN, where such Special Consumer Disclosure Requirements will be provided exclusively via electronic means; and
- Assures that each document required to be presented and/or signed is in fact presented and/or signed as required by law governing the particular transaction.

As noted further above, Users may configure the Emcee Solution to meet the regulatory requirements applicable to transactions conducted using the Emcee Solution. In fact, our view is that Users may configure the Emcee Solution to reduce the compliance risk associated with the transactions below the risk associated with similar transactions using wet ink and paper.

### ***Relative Risk***

---

<sup>33</sup> Federal Rules of Evidence 902 (11).

<sup>34</sup> *Id.* at 773 at footnote 4.

As noted throughout this letter, we believe it is important to consider the risks of a given electronic signature process in the context of the risks associated with a paper and wet ink process. Considering the risks of the electronic signature process relative to the corresponding risks associated with the paper and wet ink signature process allows Users to better assess the risks inherent in the electronic process. Our view is that the Emcee Solution is capable of being configured to reduce the risks considerably below the corresponding risks of using paper and wet ink. For example, the Emcee Solution can be configured to prevent a record from being signed by the Signer if there are any blanks in the record, prevent any document relating to a transaction from being submitted to the User unless all the required steps, including execution of or acknowledgement of receipt of all Special Consumer Disclosures, and securing documents from being altered without detection. Users may configure the Emcee Solution for various types of Signature Ceremonies to calibrate the risk mitigation approaches with the User's concerns about the various risks for the scenarios contemplated by each category of Signature Ceremony, in such a way that the User can in all likelihood configure the Emcee Solution so the electronic signature process has less risk than the paper and wet ink process.

#### **IV. Conclusion**

As with any tool, the effectiveness of the Emcee Solution depends on how the Users configure the solution to fit the risk profile for the particular documents and records to be presented, signed and archived. We believe, however, that a User who carefully considers the risks associated with the types of transactions to be processed using the Emcee Solution will be able to configure and implement an e-contracting process that is no riskier than, and in some cases, less risky than, the that same transaction using paper and wet ink.

\* \* \*

This letter is not legal advice or a legal opinion and discusses statutory, regulatory and judicial authority existing on the date hereof. We undertake no obligation and hereby disclaim any such obligation to update or otherwise revise this summary in the event of a change in applicable statutory, regulatory or judicial authority. We strongly recommend that each reader seek the advice of independent legal counsel with respect to any matter discussed herein.

Very truly yours,

Locke Lord Bissell & Liddell LLP



Patrick J. Hatfield

cc: Greg Casamento

PJH/raj

### Glossary of Terms

*Audit Trail* - means a record containing the processes and details involved in each significant step of a given transaction involving a User including, the process of each Signer accessing, completing, executing and transmitting each document to be signed in connection with the transaction, the User's process for authenticating each Signer of each document for that transaction and all documents executed or resulting from the process, all as cryptographically sealed.

*ESIGN* - means the Electronic Signatures In Global and National Commerce Act, 15 U.S.C §70001 et. seq., the federal electronic signature law.

*ESIGN Consent* - means the disclosure required by ESIGN to be provided to a Signer who is also a "consumer" as defined by ESIGN, to which that Signer must consent as a condition to the User providing one or more Special Consumer Disclosures to that Signer exclusively via electronic means, where such consent is given in a way that demonstrates the Signer's ability to reasonably access information in the electronic form the Special Consumer Disclosures will be provided.

*Signer* – means each person in a given transaction involving the User who is requested to sign a document agreeing to terms and conditions in such document, including acknowledgements of receipt, applications or requests to be considered for rights or benefits, consents to specified terms, or terms in conditions in a two or multi-party agreement for the purchase or sale of goods or services.

*Special Consumer Disclosure* - means information relating to a transaction or transactions in or affecting interstate or foreign commerce, required by a statute, regulation, or rule of law (other than ESIGN) to be provided or made available to a consumer in writing, which triggers the obligation to provide the ESIGN Disclosure.

*UETA* - the version of the Uniform Electronic Transactions Act, as published by the National Conference of Commissioners on Uniform State Laws.

*User* - means a company with whom Interlink has contracted which deploys the Emcee Solution to manage the process for that company to enter contracts with Signers.

## Attachment 1

### Feature and Functions of the Emcee Solution

The degree to which the Emcee Solution itself matches the descriptions below or allows the User to configure the Emcee Solution to match the descriptions should be considered relative to how that same User addresses each topic for process(es) using paper and wet ink.

#### Authentication Risk

1. The Audit Trail will include for each document to be signed, the steps taken, as applicable, for the User to verify the identity of the Signer. Such verification steps may include confirmation of the identity of such person from a trusted source, such as a single sign on process deployed by, or otherwise determined to be reliable by, the User or the results from an identity verification process conducted by an independent third party, such as a consumer reporting agency or other trusted third party offering such services, or the answer to a shared secret question that the User determines to adequately verify the identity of the Signer. The User determines the actual method of authenticating the identity of each person involved in a given type of transaction.
2. The identity of each Signer can be independently verified in connection with each Signer's execution of a document.
3. For documents required to be notarized, the Emcee Solution allows the notary verifying another Signer's signature to enter the notary's signature and other credentials, in accordance with applicable state notary laws.

#### Repudiation Risk

1. Simultaneously with each Signer signing a document presented by the Emcee Solution, the Emcee Solution uses industry standard encryption technology to render the signed document unalterable without detection, short of using supercomputing power for an extended period of time to un-encrypt such document.
2. Each encrypted document can be securely stored in such a way that it cannot be accessed without overcoming at least industry standard security safeguards applicable to the document in question.
3. For each transaction, whether such transaction involves two or more parties, the Emcee Solution will record the date and time of each significant step and the identity of the person taking each such step and each particular step taken by that party, where such record is part of the Audit Trail.
4. The Audit Trail for each transaction includes, without limitation, each document presented and / or signed during a given transaction where each such document signed having been encrypted as described above.

5. The Audit Trail is separately encrypted using industry standard encryption technology to render the Audit Trail unalterable without detection, short of using supercomputing power for an extended period of time to un-encrypt such document.
6. The electronic sound, symbol or process used by each Signer to demonstrate his or her intent to sign a record is attached to or logically associated with the record containing terms and conditions clearly explaining to such Signer the significance of created such sound, affixing such symbol or completing such process.

#### Admissibility Risk

1. The Emcee Solution can be configured to generate true, accurate and complete hard copies of each document signed by each Signer for each transaction that accurately reflect what the Signer was presented with in connection with each Signer using the electronic signature facility within the Emcee Solution to sign each such document.
2. The Emcee Solution can be configured to generate true, accurate and complete hard copies of the Audit Trail for each transaction.
3. The hard copies referred to in 1 above would be in plain English enabling a reasonably well educated person familiar with the underlying transactions to understand the content of each document bearing a Signer's signature.
4. The hard copies referred to in 2 above would be in plain English enabling a reasonably well educated person familiar with the underlying transactions and the steps in the process to complete the transactions to understand the content of the Audit Trail.
5. The Emcee Solution would allow the User who properly configured the Emcee Solution do to so, to testify that each hard copy described in 1 and 2 above was generated from electronic records that were cryptographically sealed in such a way that each record, as accurately represented by such hard copies, could not have been altered without detection, in the absence of a person using supercomputing power to break the encryption method used, currently thought to require several years of such supercomputing power.
6. The Emcee Solution has built-in safeguards that would not allow a User to alter documents after they are signed by a Signer and cryptographically secured.

#### Compliance Risk

1. The Emcee Solution allows the User to designate each record to be presented to the Signer in such a way that the presentation of such record matches in all material respects to the hard copy of such record designated by the User, including, all required content and the proximity of any warning, notice, disclosure or other record to be posted.

2. The Emcee Solution allows the User to designate one or more records to be presented as a “Special Consumer Disclosure” which may be provided exclusively via electronic means, but only if the Signer has affirmatively consented to receive such consumer disclosure exclusively via electronic means.
3. For each Special Consumer Disclosure, the User may configure the Emcee Solution to present the ESIGN Consent to each Signer in the same manner in which the Special Consumer Disclosures will be provided to that Signer.
4. Users may draft the ESIGN Consents to be used by the Emcee Solution that complies with the ESIGN consumer disclosure requirements.
5. If another law adopted prior to ESIGN which is applicable to a given transaction requires a document to be given by a specific method that requires verification or acknowledgement of receipt, such as registered mail return receipt required, the User may configure the Emcee Solution to require verification or acknowledgement of receipt of such document.
6. The Audit Trail records each of the 5 steps above for each transaction.

## **Attachment 2**

### **How the Emcee Solution Satisfies the Descriptions in Attachment 1**

The degree and manner in which the Emcee Solution satisfies each description in Attachment 1 is listed below:

#### **Authentication Risk**

1. The Emcee Solution permits the User to determine the level of Signer authentication to be included in a given Signing Ceremony. For Signers known to the User prior to execution of a Signing Ceremony, the Signer's credentials are passed to the Emcee Solution at the moment of execution. Upon completion of its signing transaction the Signer's credentials are securely stored and can be retrieved in relation to a transaction at any time.
2. In connection with each Signer's execution of a document, the Emcee Solution verifies the identity of a signer against the identity of the expected signer in a ceremony, based on credentials identified by the User, prior to permitting the Signer to sign.
3. In a preferred execution of a Signing Ceremony the Emcee Solution would stipulate that a notary be the last Signer to sign, thus having the benefit of examining the validity of all prior signatures.

#### **Repudiation Risk**

1. Simultaneously with each Signer signing a document using a signature image, the Emcee Solution makes use of the cryptographic infrastructure (RSA, SHA1) of Windows to create digital signatures that mathematically bind a document to a Signer.
2. The Emcee Solution makes use of the User's secure storage capabilities.
3. A Signing Ceremony, unique to the Emcee Solution, contains document, Signer and order of the steps information prior to execution. During execution all actions are time-stamped. The resulting executed Signing Ceremony is securely stored and Audit Trail reports can then be generated from it.
4. The Audit Trail may include each action that took place in chronological order as may be designated by the User. Since the Audit Trail is not a report but a database, the generation of reports about a single transaction, or a single document are as easy as global reports about all the documents and Signers involved
5. Signing Ceremonies and executed signing ceremonies are kept in encrypted secure database systems

6. A Signer is presented with affirmation steps or documents, to which he has to agree or acknowledge prior to be allowed to sign. Signer acknowledgements are also kept in executed Signing Ceremonies.

#### Admissibility Risk

1. All signed documents are in PDF format and can be verified for alterations. Audit Trails are generated from secure database records.
2. The Emcee Solution encrypts all documents using digital signatures (RSA, SHA1) exclusively.

#### Compliance Risk

1. The Emcee Solution presents all the pages of a document to the Signer in the exact form and order as a hard copy of the document as defined by the User, for each Signing Ceremony.
2. The Emcee Solution allows the User to present “Special Consumer Disclosures” and other affirmation texts, consent documents, etc., among other documents of a Signing Ceremony.
3. It is obligatory that each Signer provides his or her consent prior to signing.
4. The Emcee Solution can be configured to allow a Signer to confirm receipt of a hardcopy as part of a Signing Ceremony.