## EXHIBIT D: THE '322 PATENT INVALIDITY CLAIM CHART

| U.S. Patent No. 6,085,322 | Dziewit et al., U.S. Patent No. 5,031,214 | Bisbee et al., U.S. Patent No. 5,748,738 |
|---|---|---|
| 1. A method for establishing the authenticity of an electronic document comprising: | Claim 1 is invalid as being obvious over Dziewit in view of the prior art admitted by the '322 patent.<br><br>Dziewit teaches a method for authenticating an electronic document, and thus, for establishing the authenticity of the document. (See Col. 2:3-68 and Col. 12:44-57). | Claim 1 is invalid as being obvious over Bisbee in view of the prior art admitted by the '322 patent.<br><br>"System and Method for Electronic Transmission, Storage and Retrieval of Authenticated Documents." (Title). |
| [**a.**] obtaining an electronic document; | "The document editing process typically begins with the individual (first party) logging on to processor 134 and accessing a file." (Col. 9:24-26). "At step 302, the individual requests access to a file named document for the purpose of editing this file." (Col. 9:41-43). | "In the first step, an electronic document is designed, or drafted, that reflects the agreement of parties, such as a manufacturing operation depicted by the factory in FIG. 7." (Col. 9:29-32). |
| [**b.**] obtaining a first electronic signature indicia from an originating party; | "In such a situation, it is typical to have all the parties colocated so the witnesses can attest **to the first party signing the document** by placing their signatures electronically on the document." (Col. 12:53-57)(emphasis added).<br><br>Dziewit does not explicitly specify that the step of obtaining an electronic signature indicia from the originating party; however, this step is implicit in that the colocated parties attest to the first party signing the digital document. | "The electronic document is provided to a Transfer Agent's terminal, which is illustrated as a portable computer having an authorized Token and, optionally, a stylus pad for capturing hand-written signatures. A typical configuration for a Transfer Agent's terminal is at least the computational equivalent of a 386 desktop or laptop computer, with high resolution graphics, a Token reader, and a stylus pad for capturing hand-written signatures. As shown in FIG. 7, the electronic document, which may be created locally or remotely, is displayed on this terminal." (Col. 9:32-41) |

| U.S. Patent No. 6,085,322 | Dziewit et al., U.S. Patent No. 5,031,214 | Bisbee et al., U.S. Patent No. 5,748,738 |
|---|---|---|
| | | "In the second step, the parties to the agreement execute their hand-written signatures on the document using the stylus pad. These signatures are captured and inserted in appropriate locations in the electronic document." (Col. 9:42-49). |
| [c.] applying said first electronic signature indicia to said electronic document; | See claim 1b.<br><br>"Once validation of the identification of all contracting parties is obtained, then the file 'document' is 'signed' by all the parties and the legal document has been executed electronically." (Col. 12:48-51).<br><br>"The actual 'signing' or authenticating of the electronic document can be implemented as an additional password step utilizing personnel identity validation apparatus." (Col. 2:35-38).<br><br>"The authentication of the document by the contracting parties consummates the execution of the document. The document authentication apparatus responds to the authentication operation by providing sufficient safeguards to insure that the contents of the file have not been modified or altered following the consummation of the multi-party contract single party document without the alteration being detectable. This is typically accomplished by the generation of a 'digital | See claim 1b.<br><br>"In the second step, the parties to the agreement execute their hand-written signatures on the document using the stylus pad. These signatures are captured and inserted in appropriate locations in the electronic document." (Col. 9:42-49). |

| U.S. Patent No. 6,085,322 | Dziewit et al., U.S. Patent No. 5,031,214 | Bisbee et al., U.S. Patent No. 5,748,738 |
|---|---|---|
| | signature' that 'fingerprints' the document such that not even a single bit of the document can be altered without this change being reflected in the digital signature." (Col. 2:47-58). | |
| [**d.**] generating an identification envelope comprising a verifying statement, said verifying statement comprising a statement by a verifying party indicating that said verifying party witnessed the application of said first electronic signature indicia; | "In such a situation, it is typical to have all the **parties colocated** so the **witnesses can attest** to the first party signing the document by placing their signatures electronically on the document." (Col. 12:53-57)(emphasis added).<br><br>Dziewit does not explicitly specify the existence of a *verifying statement*; however, the presence of such a statement must inherently exist since the witnesses attest to witnessing the signing of the electronic document. This "attestation" is a *verifying statement*. Moreover, the '322 patent itself admits to the routine nature of a *verifying statement* in prior art Notarial practice. (Col. 1:18-25).<br><br>Dziewit does not teach the creation of an *identification envelope*, but the '322 patent itself admits to such statements being routine in standard Notarial practice. Specifically, in its description of the prior art, the '322 patent teaches: "For certain transactions, authentication of a handwritten signature, for example by a licensed public official such as a notary, is required. Authentication of a | "After all parties have signed the document, the Transfer Agent **certifies the completion of the document's execution** by invoking his or her digital signature and appending his or her certificate, using the Token." (Col. 9:41-49)(emphasis added).<br><br>"The DAS also would permit a 'Notary Public' type of secondary support function. This would permit a third party present at the document's execution to also have a cryptographic card which would "seal" the transaction for further verification that the parties executing or sealing the document to be signed were in fact the proper parties. This additional notary function is not required, but would assist in the further authentication of the identities of the parties." (Col. 8:55-62). (This teaching also exists in the '738 patent considered during prosecution of the Romney patents).<br><br>Bisbee does not teach the creation of an *identification envelope*, but the '322 patent itself admits to such statements being routine in standard Notarial practice. Specifically, in its description of |

| U.S. Patent No. 6,085,322 | Dziewit et al., U.S. Patent No. 5,031,214 | Bisbee et al., U.S. Patent No. 5,748,738 |
|---|---|---|
| | signature by a notary requires a personal appearance before the notary. The notary personally witnesses the execution of the signature, inspects identity documents to verify the identity of the person executing the signature, and **affixes a notary statement and seal to the signed document**." (Col. 1:21-28)(emphasis added). Thus, it would have been obvious to one of skill in the art to include an *identification envelope* when the co-located witnessing party of Dziewit is a Notary. | the prior art, the '322 patent teaches: "For certain transactions, authentication of a handwritten signature, for example by a licensed public official such as a notary, is required. Authentication of a signature by a notary requires a personal appearance before the notary. The notary personally witnesses the execution of the signature, inspects identity documents to verify the identity of the person executing the signature, and **affixes a notary statement and seal to the signed document**." (Col. 1:18-25)(emphasis added). Thus, it would have been obvious to one of skill in the art to include an *identification envelope* in the system of Bisbee. |
| [**e.**] obtaining a second electronic signature indicia from said verifying party; | "In such a situation, it is typical to have all the parties colocated so the **witnesses can attest** to the first party signing the document **by placing their signatures electronically on the document**." (Col. 12:53-57)(emphasis added). | "The electronic document is provided to a Transfer Agent's terminal, which is illustrated as a portable computer having an authorized Token and, optionally, a stylus pad for capturing hand-written signatures. A typical configuration for a Transfer Agent's terminal is at least the computational equivalent of a 386 desktop or laptop computer, with high resolution graphics, a Token reader, and a stylus pad for capturing hand-written signatures. As shown in FIG. 7, the electronic document, which may be created locally or remotely, is displayed on this terminal." (Col. 9:32-41)<br><br>"In the second step, the parties to the agreement |

| U.S. Patent No. 6,085,322 | Dziewit et al., U.S. Patent No. 5,031,214 | Bisbee et al., U.S. Patent No. 5,748,738 |
|---|---|---|
| | | execute their hand-written signatures on the document using the stylus pad. These signatures are captured and inserted in appropriate locations in the electronic document." (Col. 9:42-49).<br><br>"After all parties have signed the document, the Transfer Agent **certifies the completion of the document's execution** by invoking his or her digital signature and appending his or her certificate, using the Token." (Col. 9:41-49)(emphasis added). |
| [**f.**] applying said second electronic signature indicia to said electronic document. | "In such a situation, it is typical to have all the parties colocated so the **witnesses can attest** to the first party signing the document **by placing their signatures electronically on the document.**" (Col. 12:53-57)(emphasis added). | See claim 1e.<br><br>"In the second step, the parties to the agreement execute their hand-written signatures on the document using the stylus pad. These signatures are captured and inserted in appropriate locations in the electronic document." (Col. 9:42-49).<br><br>"After all parties have signed the document, the Transfer Agent **certifies the completion of the document's execution** by invoking his or her digital signature and appending his or her certificate, using the Token." (Col. 9:41-49)(emphasis added). |
| **2.** The method of claim 1 wherein said first electronic | Claim 2 is invalid as being obvious over Dziewit in view of the prior art admitted by the '322 patent. | Claim 2 is invalid as being obvious over Bisbee in view of the prior art admitted by the '322 patent. |

| U.S. Patent No. 6,085,322 | Dziewit et al., U.S. Patent No. 5,031,214 | Bisbee et al., U.S. Patent No. 5,748,738 |
|---|---|---|
| signature indicia is obtained from said originating party using an electronic input device. | In such a situation, it is typical to have all the parties colocated so the witnesses can attest to the first party signing the document by placing their signatures electronically on the document." (Col. 12:53-57).<br><br>"At step 322, personnel identification process 205 enables and scans a sensor (ex. device 142) associated with the first party. The sensors, as described above, can be as elemental as a prompt to the terminal associated with the selected party to enter a password that is theoretically known only to the selected party. The accuracy of personnel identity validation can be improved by the addition of various peripheral devices 142, 141 that measure some immutable physical characteristic of the party. These devices include fingerprint scanners, voiceprint identifiers, retina scanners, etc." (Col. 12:15-26).<br><br>Dziewit teaches that the parties place their signatures electronically on the document, and teaches the use of electronic input devices for the collection of biometric data. To the extent such devices are not inherently present in Dziewit, it would have been obvious to modify Dziewit to include an electronic device for recording an electronic signature indicia. | "In the second step, the parties to the agreement execute their hand-written signatures on the document using the stylus pad. These signatures are captured and inserted in appropriate locations in the electronic document." (Col. 9:42-49). |

| U.S. Patent No. 6,085,322 | Dziewit et al., U.S. Patent No. 5,031,214 | Bisbee et al., U.S. Patent No. 5,748,738 |
|---|---|---|
| **3.** The method of claim 1 wherein said identification envelope comprises biometric data obtained from said originating party. | Claim 3 is invalid as being obvious over Dziewit in view of the prior art admitted by the '322 patent.<br><br>"In either case, the personnel identification process is initiated at step 321 by the individual (first party) to be bound by the file "document" assenting to the form and content of the file "document" as is presently stored in the document authentication software 143. The assent is obtained by personnel identification process 205 polling the individual (first party) to obtain initial confirmation that authentication is appropriate. At step 322, personnel identification process 205 enables and scans a sensor (ex. device 142) associated with the first party. The sensors, as described above, can be as elemental as a prompt to the terminal associated with the selected party to enter a password that is theoretically known only to the selected party. The accuracy of personnel identity validation can be improved by the addition of various peripheral devices 142, 141 that measure some immutable physical characteristic of the party. These devices include fingerprint scanners, voiceprint identifiers, retina scanners, etc." (Col. 12:8-26).<br><br>The '322 patent teaches: "The notary personally witnesses the execution of the signature, inspects identity documents to verify the identity of the | Claim 3 is invalid as being obvious over Bisbee in view of the prior art admitted by the '322 patent.<br><br>"In an additional aspect of Applicant's invention, the public/private key is only effective when it is used in conjunction with a certificate and personal identification information such as the recipient's biometric information (e.g., retina-, finger-, and voice-prints) or a personal identification number (PIN) that is assigned to the recipient of the card by the Certification Authority and that may be delivered separate from the originator's card." (Col. 4:61 - Col. 5:1).<br><br>"The notary personally witnesses the execution of the signature, inspects identity documents to verify the identity of the person executing the signature, and affixes a notary statement and seal to the signed document." ('322 at Col. 1:21-25).<br><br>Thus, the '322 patent admits that prior art Notarial processes involve the inspection of identity documents. Bisbee teaches the use of biometric data as a means of using a digital signature. To ensure proper identification of the originating party, it would have been obvious to modify Bisbee to record the biometric data to identify the originating party, and to include that information in the |

| U.S. Patent No. 6,085,322 | Dziewit et al., U.S. Patent No. 5,031,214 | Bisbee et al., U.S. Patent No. 5,748,738 |
|---|---|---|
| | person executing the signature, and affixes a notary statement and seal to the signed document." ('322 at Col. 1:21-25).<br><br>Thus, the '322 patent admits that prior art Notarial processes involve the inspection of identity documents. Dziewit teaches the use of biometric data for identification purposes. To ensure proper identification of the originating party, it would have been obvious to modify Dziewit to record the biometric data and to include that information in the identification envelope. | identification envelope. |
| **4.** The method of claim 3 wherein said biometric data comprises a retinal eye scan obtained from said originating party. | Claim 4 is invalid as being obvious over Dziewit in view of the prior art admitted by the '322 patent.<br><br>See claim 3.<br><br>"These devices include fingerprint scanners, voiceprint identifiers, **retina scanners**, etc." (Col. 12:24-26)(emphasis added). | Claim 4 is invalid as being obvious over Bisbee in view of the prior art admitted by the '322 patent.<br><br>See claim 3.<br><br>"In an additional aspect of Applicant's invention, the public/private key is only effective when it is used in conjunction with a certificate and personal identification information such as the recipient's biometric information (e.g., **retina-**, finger-, and voice-**prints**) or a personal identification number (PIN) that is assigned to the recipient of the card by the Certification Authority and that may be delivered separate from the originator's card." (Col. 4:61 - Col. 5:1) (emphasis added). |

| U.S. Patent No. 6,085,322 | Dziewit et al., U.S. Patent No. 5,031,214 | Bisbee et al., U.S. Patent No. 5,748,738 |
|---|---|---|
| **5.** The method of claim 3 wherein said biometric data comprises a digitized fingerprint obtained from said originating party. | Claim 5 is invalid as being obvious over Dziewit in view of the prior art admitted by the '322 patent.<br><br>See claim 3.<br><br>"These devices include **fingerprint scanners**, voiceprint identifiers, retina scanners, etc." (Col. 12:24-26)(emphasis added). | Claim 5 is invalid as being obvious over Bisbee in view of the prior art admitted by the '322 patent.<br><br>See claim 3.<br><br>"In an additional aspect of Applicant's invention, the public/private key is only effective when it is used in conjunction with a certificate and personal identification information such as the recipient's biometric information (e.g., retina-, **finger-**, and voice-**prints**) or a personal identification number (PIN) that is assigned to the recipient of the card by the Certification Authority and that may be delivered separate from the originator's card." (Col. 4:61 - Col. 5:1)(emphasis added). |
| **6.** The method of claim 1 wherein said identification envelope comprises a public key of said originating party. | Claim 6 is invalid as being obvious over Dziewit in view of the prior art admitted by the '322 patent.<br><br>"A more secure and complex system that minimizes the possibility of fraud by the contracting parties is the RSA Public Key Cryptosystem. This system uses two encryption keys. A "private key" is used by the document sender to scramble the data while a "public key", known to the document recipient, is used to decode the received document." (Col. 7:6-12).<br><br>The '322 patent teaches that a party "freely | Claim 6 is invalid as being obvious over Bisbee in view of the prior art admitted by the '322 patent.<br><br>"In one aspect of Applicant's invention, a method of authenticating an electronic document comprises the steps of: signing the electronic document with a digital signature of a Transfer Agent; appending a certificate to the electronic document by the Transfer Agent; and validating the digital signature and certificate of the Transfer Agent. The certificate may include information representing the Transfer Agent's identity, public cryptographic key, and predetermined attributes." (Col. 30-37). |

| U.S. Patent No. 6,085,322 | Dziewit et al., U.S. Patent No. 5,031,214 | Bisbee et al., U.S. Patent No. 5,748,738 |
|---|---|---|
| | distributes its public key." (Col. 2:20-21). Thus, it would have been obvious to include a copy of the originating parties public key in the identification envelope. | The '322 patent teaches that a party "freely distributes its public key." (Col. 2:20-21). Thus, it would have been obvious to include a copy of the originating parties public key in the identification envelope. |
| **7.** The method of claim 1 wherein said identification envelope comprises a digital certificate of said originating party. | Claim 7 is invalid as being obvious over Dziewit in view of the prior art admitted by the '322 patent.<br><br>"Digital encryption, digital message digests, digital signatures, and digital certificates are some of the existing cryptographic tools that are used in the present invention to address this need." ('322 at Col. 1:49-52). "Digital signatures and digital certificates have been devised to address some of the uncertainties inherent in public key cryptography." ('322 at Col. 2:56-58). "Digital certificates are intended to provide a level of assurance as to the identity of the holder of the private key corresponding to a particular public key. The issuers of digital certificates are called certification authorities. A digital certificate constitutes a certification by a certification authority that a particular public key is the public key of a particular entity, and that this entity is the holder of the corresponding private key." ('322 at Col. 3:35-43). "The authenticity of a digital certificate is tested by verifying the certification authority's digital signature using the certification | Claim 7 is invalid as being obvious over Bisbee in view of the prior art admitted by the '322 patent.<br><br>"In one aspect of Applicant's invention, a method of authenticating an electronic document comprises the steps of: signing the electronic document with a digital signature of a Transfer Agent; appending a certificate to the electronic document by the Transfer Agent; and validating the digital signature and certificate of the Transfer Agent. The certificate may include information representing the Transfer Agent's identity, public cryptographic key, and predetermined attributes." (Col. Col. 3:3-10).<br><br>"Issuance by the Certification Authority of a digitally signed certificate ensures the verifiability of the identity of each transmitter of a digitally signed or encrypted document." (Col. 5:15-17).<br><br>Bisbee teaches the step of appending the digital certificate to an electronic document. It would have been obvious to include the digital certificate in the "identification envelope". |

| U.S. Patent No. 6,085,322 | Dziewit et al., U.S. Patent No. 5,031,214 | Bisbee et al., U.S. Patent No. 5,748,738 |
|---|---|---|
| | authority's public key." ('322 at Col. 3:64-66). "The digital certificate may be appended to an electronic document, or the recipient of an electronic document may obtain a copy of the certificate from the issuing certification authority or other certificate repository." ('322 at Col. 4:13-17).<br><br>The '322 patent admits that the use of digital certificates to link a party to a digital signature was common in the prior art. Thus, it would have been obvious to include a digital certificate in the method of Dziewit to verify ownership of the private/public key pair associated with the digital signature. | |
| **8.** The method of claim 1 wherein said identification envelope comprises a digital certificate of said verifying party. | Claim 8 is invalid as being obvious over Dziewit in view of the prior art admitted by the '322 patent.<br><br>See Claim 7. | Claim 8 is invalid as being obvious over Bisbee in view of the prior art admitted by the '322 patent.<br><br>See claim 7. |
| **9.** The method of claim 1 further comprising: | Claim 9 is invalid as being obvious over Dziewit in view of the prior art admitted by the '322 patent and U.S.P. 5,005,200. | Claim 9 is invalid as being obvious over Bisbee in view of the prior art admitted by the '322 patent and U.S.P. 5,005,200. |
| delineating said identification envelope with indicators; | The technique of "appending indicators" to an electronic document to delineate various sections of the document, such as "main text" and "digital signature is notoriously old. See, for example, | The technique of "appending indicators" to an electronic document to delineate various sections of the document, such as "main text" and "digital signature is notoriously old. See, for example, |

| U.S. Patent No. 6,085,322 | Dziewit et al., U.S. Patent No. 5,031,214 | Bisbee et al., U.S. Patent No. 5,748,738 |
|---|---|---|
| | Figure 8 of U.S.P. 5,005,200. It would have been obvious to include in the Dziewit method the step of appending indicators to delineate the identification from the signed document. | Figure 8 of U.S.P. 5,005,200. It would have been obvious to include in the Bisbee method the step of appending indicators to delineate the identification from the signed document. |
| identifying materials used by said verifying party to verify the identity of said originating party. | "The notary personally witnesses the execution of the signature, inspects identity documents to verify the identity of the person executing the signature, and affixes a notary statement and seal to the signed document." ('322 at Col. 1:21-25).<br><br>The '322 patent admits that prior art Notarial processes involve the inspection of identity documents. It would have been obvious to include in the identification envelope information identifying which documents were inspected. | "The notary personally witnesses the execution of the signature, inspects identity documents to verify the identity of the person executing the signature, and affixes a notary statement and seal to the signed document." ('322 at Col. 1:21-25).<br><br>The '322 patent admits that prior art Notarial processes involve the inspection of identity documents. It would have been obvious to include in the identification envelope information identifying which documents were inspected. |
| **10.** The method of claim 1 wherein said identification envelope is computer encoded. | Claim 10 is invalid as being obvious over Dziewit in view of the prior art admitted by the '322 patent.<br><br>The '322 patent provides limited explanation for what is meant by "computer encoded". In fact, the only mention of the term, outside the claims, is: "An authenticator statement may be in a human language or may be computer encoded." (Col. 9:32-33). Non-human language documents are notoriously old in the field of electronic documents -- in fact, all electronic documents are preserved as digital data in a non-human-readable format. Thus, | Claim 10 is invalid as being obvious over Bisbee in view of the prior art admitted by the '322 patent.<br><br>The '322 patent provides limited explanation for what is meant by "computer encoded". In fact, the only mention of the term, outside the claims, is: "An authenticator statement may be in a human language or may be computer encoded." (Col. 9:32-33). Non-human language documents are notoriously old in the field of electronic documents -- in fact, all electronic documents are preserved as digital data in a non-human-readable format. Thus, |

| U.S. Patent No. 6,085,322 | Dziewit et al., U.S. Patent No. 5,031,214 | Bisbee et al., U.S. Patent No. 5,748,738 |
|---|---|---|
| | it would have been obvious to computer encode the identification. | it would have been obvious to computer encode the identification. |
| **11.** The method of claim 1 wherein said first electronic signature indicia comprises a first digital signature. | Claim 11 is invalid as being obvious over Dziewit in view of the prior art admitted by the '322 patent.<br><br>"In such a situation, it is typical to have all the parties colocated so the witnesses can attest **to the first party signing the document** by placing their signatures electronically on the document." (Col. 12:53-57)(emphasis added).<br><br>"Once validation of the identification of all contracting parties is obtained, then the file 'document' is 'signed' by all the parties and the legal document has been executed electronically." (Col. 12:48-51).<br><br>"The actual 'signing' or authenticating of the electronic document can be implemented as an additional password step utilizing personnel identity validation apparatus." (Col. 2:35-38).<br><br>"The authentication of the document by the contracting parties consummates the execution of the document. The document authentication apparatus responds to the authentication operation by providing sufficient safeguards to insure that the contents of the file have not been modified or | Claim 11 is invalid as being obvious over Bisbee in view of the prior art admitted by the '322 patent.<br><br>"In the second step, the parties to the agreement execute their hand-written signatures on the document using the stylus pad. These signatures are captured and inserted in appropriate locations in the electronic document. After all parties have signed the document, the Transfer Agent certifies the completion of the document's execution by invoking his or her digital signature and appending his or her certificate, using the Token. " (Col. 9:41-49).<br><br>Bisbee teaches the use of digitized *electronic signatures* rather than *digital signatures*. However, the *electronic signature* genus includes the *digital signature* species. Moreover, both Bisbee and the '322 patent admit to the need for digital signatures to preserve the integrity of an electronic document. (Bisbee at Col. 2:11-61 and Col. 9:45-49; '322 patent at Col. 2:56-64). To better assure the integrity of an electronic document, one of skill in the art would have been motivated to use *digital signatures* in place of the digitized *electronic signatures* of Bisbee. |

| U.S. Patent No. 6,085,322 | Dziewit et al., U.S. Patent No. 5,031,214 | Bisbee et al., U.S. Patent No. 5,748,738 |
|---|---|---|
| | altered following the consummation of the multi-party contract single party document without the alteration being detectable. This is typically accomplished by the generation of a 'digital signature' that 'fingerprints' the document such that not even a single bit of the document can be altered without this change being reflected in the digital signature." (Col. 2:47-58).<br><br>Dziewit is ambiguous as to whether the co-located parties sign the electronic document with *digital signatures* or *electronic signatures* (such as a *digitized signature*). To the extent the parties use *digital signatures*, the *digital signatures* limitation of claim 10 is explicitly taught by Dziewit. If the Dziewit signatures are *electronic signatures*, the *digital signatures* limitation of claim 10 is rendered obvious by Dziewit. The definition of *electronic signatures* includes *digital signatures*. Both Dziewit and the '322 patent admit to the need for digital signatures to preserve the integrity of an electronic document. (Dziewit at Col. 12:62-67; '322 patent at Col. 2:56-64). To better assure the integrity of an electronic document, one of skill in the art would have been motivated to use *digital signatures* in place of the *electronic signatures* of the co-located parties taught by Dziewit. | |
| **12.** The method of claim 1 | Claim 12 is invalid as being obvious over Dziewit | Claim 12 is invalid as being obvious over Bisbee in |

| U.S. Patent No. 6,085,322 | Dziewit et al., U.S. Patent No. 5,031,214 | Bisbee et al., U.S. Patent No. 5,748,738 |
|---|---|---|
| wherein said first electronic signature indicia is manually entered by said originating party. | in view of the prior art admitted by the '322 patent.<br><br>The '322 patent does not specify what is meant by the electronic signature indicia being "manually entered". But see claims 1, 2, and 11. | view of the prior art admitted by the '322 patent.<br><br>The '322 patent does not specify what is meant by the electronic signature indicia being "manually entered". But see claims 1, 2, and 11. |
| **13.** The method of claim 1 wherein said second electronic signature indicia comprises a second digital signature. | Claim 13 is invalid as being obvious over Dziewit in view of the prior art admitted by the '322 patent.<br><br>See claim 11. | Claim 13 is invalid as being obvious over Bisbee in view of the prior art admitted by the '322 patent.<br><br>See claim 11. |
| **14.** The method of claim 1 wherein said second electronic signature indicia is manually entered by said verifying party. | Claim 14 is invalid as being obvious over Dziewit in view of the prior art admitted by the '322 patent.<br><br>See claim 12. | Claim 14 is invalid as being obvious over Bisbee in view of the prior art admitted by the '322 patent.<br><br>See claim 12. |