IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

TQP DEVELOPMENT, LLC

Plaintiff,

v.

(1) BARCLAYS PLC;
(2) BARCLAYS BANK PLC;
(3) BARCLAYS BANK DELAWARE, F/K/A JUNIPER FINANCIAL MANAGEMENT, INC.;
(4) BARCLAYS ELECTRONIC COMMERCE HOLDINGS INC.;
(5) BARCLAYS CAPITAL INC.;
(6) PRUDENTIAL FINANCIAL INC.;
(7) THE PRUDENTIAL INSURANCE COMPANY OF AMERICA;
(8) PRUCO SECURITIES, LLC;
(9) PRUCO SECURITIES CORPORATION;
(10) AMAZON.COM, INC;
(11) VISA INC;
(12) VISA USA INC;
(13) VISA INTERNATIONAL SERVICE ASSOCIATION;
(14) AMERICAN EXPRESS COMPANY;
(15) AMERICAN EXPRESS TRAVEL RELATED SERVICES;
(16) MASTERCARD INC; AND
(17) MASTERCARD INTERNATIONAL, LLC,

Defendants.

Civil Action No. 2:09-cv-00088

JURY TRIAL DEMANDED

<u>COMPLAINT FOR PATENT INFRINGEMENT</u>

This is an action for patent infringement in which TQP Development, LLC ("TQP"). makes the following allegations against Barclays PLC; Barclays Bank PLC; Barclays Bank

Delaware, f/k/a Juniper Financial Management, Inc.; Barclays Electronic Commerce Holdings Inc.; Barclays Capital Inc; Prudential Financial Inc.; The Prudential Insurance Company of America; Pruco Securities, LLC; Pruco Securities Corporation; Amazon.com, Inc; Visa Inc; Visa USA Inc; Visa International Service Association; American Express Company; American Express Travel Related Services; MasterCard Inc; and MasterCard International, LLC (collectively the "Defendants").

PARTIES

1. Plaintiff TQP Development, LLC is a Texas limited liability company having a principal place of business of 207C North Washington Ave., Marshall, TX 75670.

2. On information and belief, Defendant Barclays PLC ("Barclays") is a United Kingdom corporation with its principal place of business at 1 Churchill Place, London, E14 5HP, United Kingdom. Barclays has appointed Patrick Gonsalves located at 1 Churchill Place, London, E14 5HP, United Kingdom, as its agent for service of process.

3. On information and belief, Defendant Barclays Bank PLC ("Barclays Bank") is a United Kingdom corporation with its principal place of business at 1 Churchill Place, London, E14 5HP, United Kingdom. Barclays Bank has appointed Patrick Gonsalves located at 1 Churchill Place, London, E14 5HP, United Kingdom, as its agent for service of process.

4. On information and belief, Defendant Barclays Bank Delaware, f/k/a Juniper Financial Management, Inc. ("Barclays Delaware") is a Delaware corporation with its principal place of business at 100 S. West St., Wilmington, DE 19801. Barclays Delaware has appointed Corporation Trust Company located at Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801, as its agent for service of process.

5. On information and belief, Defendant Barclays Electronic Commerce Holdings

Inc. ("Barclays Electronic") is a Delaware corporation with its principal place of business at 5 The North Colonnade, Canary Wharf, London, E14 4BB, United Kingdom. Barclays Electronic has appointed Corporation Trust Company located at Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801, as its agent for service of process.

6. On information and belief, Defendant Barclays Capital Inc. ("Barclays Capital") is a Delaware corporation with its principal place of business at 5 The North Colonnade, Canary Wharf, London, E14 4BB, United Kingdom. Barclays Capital has appointed Corporation Trust Company located at Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801, as its agent for service of process.

7. On information and belief, Defendant Prudential Financial Inc. ("Prudential") is a New Jersey corporation with its principal place of business at 751 Broad St., Newark, NJ 07102-3777. Prudential has appointed Kathleen M. Gibson located at 751 Broad St., Newark, NJ 07102-3777, as its agent for service of process.

8. On information and belief, Defendant The Prudential Insurance Company of America ("Prudential Insurance") is a New Jersey corporation with its principal place of business at 751 Broad St., Newark, NJ 07102-3777. Prudential Insurance has appointed Kathleen M. Gibson located at 751 Broad St., Newark, NJ 07102-3777, as its agent for service of process.

9. On information and belief, Defendant Pruco Securities, LLC. ("Pruco") is a New Jersey corporation with its principal place of business at 213 Washington St., Newark, NJ 07102-2917. Pruco has appointed Corporation Trust Company located at 820 Bear Tavern Road, West Trenton, NJ 08628, as its agent for service of process.

10. On information and belief, Defendant Pruco Securities Corporation. ("Pruco Corp") is a New Jersey corporation with its principal place of business at 213 Washington St.,

Newark, NJ 07102-2917. Pruco Corp has appointed Richard Topp located at 751 Broad St., Newark, NJ 07102-3777, as its agent for service of process.

11. On information and belief, Defendant Amazon.com, Inc. ("Amazon.com") is a Washington corporation with its principal place of business at 1200 12th Ave. South, Suite 1200, Seattle, WA 98144-2734. Amazon.com has appointed Corporation Trust Company located at Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801, as its agent for service of process.

12. On information and belief, Defendant Visa Inc. ("Visa") is a Delaware corporation with its principal place of business at 900 Metro Center Blvd., Foster City, CA 94404. Visa has appointed The Corporation Trust Company, Corporation Trust Center located at 1209 Orange Street, Wilmington, DE 19801, as its agent for service of process.

13. On information and belief, Defendant Visa USA Inc. ("Visa USA") is a Delaware corporation with its principal place of business at 900 Metro Center Blvd., Foster City, CA 94404. Visa USA is qualified to do business in the State of Texas and has appointed CT Corporation System located at 350 N. St. Paul Street, Dallas, TX 75201, as its agent for service of process.

14. On information and belief, Defendant Visa International Service Association. ("Visa Int'l") is a California corporation with its principal place of business at 900 Metro Center Blvd., Foster City, CA 94404. Visa Int'l has appointed The Corporation Trust Company, Corporation Trust Center located at 1209 Orange Street, Wilmington, DE 19801, as its agent for service of process.

15. On information and belief, Defendant American Express Company ("AMEX") is a New York corporation with its principal place of business at the World Financial Center, 200

Vesey St., New York, NY 10285-4415. AMEX is qualified to do business in the State of Texas and has appointed Robert H. Seberle located at the World Financial Center, 200 Vesey St., New York, NY 10285-4415, as its agent for service of process.

16. On information and belief, Defendant American Express Travel Related Services ("AMEX Travel") is a New York corporation with its principal place of business at the World Financial Center, 200 Vesey St., New York, NY 10285-4415. AMEX Travel is qualified to do business in the State of Texas and has appointed Robert H. Seberle located at the World Financial Center, 200 Vesey St., New York, NY 10285-4415, as its agent for service of process.

17. On information and belief, Defendant MasterCard Inc. ("MasterCard") is a Delaware corporation with its principal place of business 2000 Purchase Street, Purchase, NY 10577. MasterCard has appointed The Corporation Trust Company located at Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801, as its agent for service of process.

18. On information and belief, Defendant MasterCard International, LLC ("MasterCard Int'l") is a Delaware corporation with its principal place of business at 2200 MasterCard Blvd., Fallon, MO 63366. MasterCard Int'l has appointed The Corporation Trust Company located at Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801, as its agent for service of process.

JURISDICTION AND VENUE

19. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

20. Venue is proper in this district under 28 U.S.C. §§ 1391(c) and 1400(b). On information and belief, each Defendant has transacted business in this district, and has

committed and/or induced acts of patent infringement in this district.

21. On information and belief, Defendants are subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to their substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

COUNT I

INFRINGEMENT OF U.S. PATENT NO. 5,412,730

22. Plaintiff is the owner by assignment of United States Patent No. 5,412,730 ("the '730 Patent") entitled "Encrypted Data Transmission System Employing Means for Randomly Altering the Encryption Keys." The '730 Patent issued on May 2, 1995. A true and correct copy of the '730 Patent is attached as Exhibit A.

23. Upon information and belief, Defendant Barclays has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various websites (including, without limitation to, clientaccountaccess.com, ecommerce.barcap.com, juniper.com, barclaycardus.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. Without limitation, when Barclays and/or Barclays's customers connect to Barclays's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is

transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Barclays's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Barclays provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Barclays generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Barclays encrypts data for transmission from the host server to the client. In addition, Barclays directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Barclays generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Barclays decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Barclays is thus liable for infringement of the ‘730 Patent pursuant to 35 U.S.C. § 271.

24. Upon information and belief, Defendant Barclays Bank has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the ‘730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various websites (including, without limitation to, clientaccountaccess.com, ecommerce.barcap.com, juniper.com, barclaycardus.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the ‘730 Patent to the injury of TQP. Without limitation, when Barclays Bank and/or Barclays Bank’s customers connect to Barclays Bank’s website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Barclays Bank’s website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Barclays Bank provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Barclays Bank generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to

encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Barclays Bank encrypts data for transmission from the host server to the client. In addition, Barclays Bank directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Barclays Bank generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Barclays Bank decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Barclays Bank is thus liable for infringement of the ‘730 Patent pursuant to 35 U.S.C. § 271.

25. Upon information and belief, Defendant Barclays Delaware has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the ‘730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various websites (including, without limitation to, juniper.com, barclaycardus.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or

more claims of the ‘730 Patent to the injury of TQP. Without limitation, when Barclays Delaware and/or Barclays Delaware’s customers connect to Barclays Delaware’s website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Barclays Delaware’s website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Barclays Delaware provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Barclays Delaware generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Barclays Delaware encrypts data for transmission from the host server to the client. In addition, Barclays Delaware directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Barclays Delaware generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Barclays Delaware decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Barclays Delaware is thus liable for infringement of the ‘730 Patent pursuant to 35 U.S.C. § 271.

26. Upon information and belief, Defendant Barclays Electronic has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the ‘730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various websites (including, without limitation to, ecommerce.barcap.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the ‘730 Patent to the injury of TQP. Without limitation, when Barclays Electronic and/or Barclays Electronic's customers connect to Barclays Electronic's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Barclays Electronic's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the

claimed encryption algorithm under the direction of the host server. Barclays Electronic provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Barclays Electronic generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Barclays Electronic encrypts data for transmission from the host server to the client. In addition, Barclays Electronic directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Barclays Electronic generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Barclays Electronic decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Barclays Electronic is thus liable for infringement of the ‘730 Patent pursuant to 35 U.S.C. § 271.

27. Upon information and belief, Defendant Barclays Capital has been and now is

directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the ‘730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various websites (including, without limitation to, clientaccountaccess.com, ecommerce.barcap.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the ‘730 Patent to the injury of TQP. Without limitation, when Barclays Capital and/or Barclays Capital's customers connect to Barclays Capital's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Barclays Capital's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Barclays Capital provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Barclays Capital generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Barclays Capital encrypts data for transmission from the host server to the client. In addition, Barclays Capital directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Barclays Capital generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Barclays Capital decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Barclays Capital is thus liable for infringement of the ‘730 Patent pursuant to 35 U.S.C. § 271.

28. Upon information and belief, Defendant Prudential has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the ‘730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various websites (including, without limitation to, prudential.com, pruco.fccaccessonline.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the ‘730 Patent to the injury of TQP. Without limitation, when Prudential and/or Prudential’s customers connect to Prudential’s website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the

host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Prudential's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Prudential provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Prudential generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Prudential encrypts data for transmission from the host server to the client. In addition, Prudential directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Prudential generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Prudential decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Prudential is thus liable for infringement of the ‘730 Patent pursuant to 35 U.S.C. § 271.

29. Upon information and belief, Defendant Prudential Insurance has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the ‘730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various websites (including, without limitation to, prudential.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the ‘730 Patent to the injury of TQP. Without limitation, when Prudential Insurance and/or Prudential Insurance’s customers connect to Prudential Insurance’s website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Prudential Insurance’s website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Prudential Insurance provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Prudential Insurance generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the

encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Prudential Insurance encrypts data for transmission from the host server to the client. In addition, Prudential Insurance directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Prudential Insurance generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Prudential Insurance decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Prudential Insurance is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

30. Upon information and belief, Defendant Pruco has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various websites (including, without limitation to, pruco.fccaccessonline.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. Without limitation, when Pruco and/or Pruco's customers connect

to Pruco's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Pruco's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Pruco provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Pruco generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Pruco encrypts data for transmission from the host server to the client. In addition, Pruco directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Pruco generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Pruco decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Pruco is thus liable for infringement of the ‘730 Patent pursuant to 35 U.S.C. § 271.

31. Upon information and belief, Defendant Pruco Corp has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the ‘730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various websites (including, without limitation to, pruco.fccaccessonline.com for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the ‘730 Patent to the injury of TQP. Without limitation, when Pruco Corp and/or Pruco Corp’s customers connect to Pruco Corp’s website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Pruco Corp’s website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Pruco Corp provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Pruco Corp generates,

or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Pruco Corp encrypts data for transmission from the host server to the client. In addition, Pruco Corp directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Pruco Corp generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Pruco Corp decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Pruco Corp is thus liable for infringement of the ‘730 Patent pursuant to 35 U.S.C. § 271.

32. Upon information and belief, Defendant Amazon.com has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the ‘730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various websites (including, without limitation to, Amazon.com) for transmitting data comprising a

sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. Without limitation, when Amazon.com and/or Amazon.com's customers connect to Amazon.com's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Amazon.com's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Amazon.com provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Amazon.com generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Amazon.com encrypts data for transmission from the host server to the client. In addition, Amazon.com directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Amazon.com generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Amazon.com decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Amazon.com is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

33. Upon information and belief, Defendant Visa has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various websites (including, without limitation to, visaextras.com, visa.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. Without limitation, when Visa and/or Visa's customers connect to Visa's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Visa's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Visa

provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Visa generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Visa encrypts data for transmission from the host server to the client. In addition, Visa directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Visa generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Visa decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Visa is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

34. Upon information and belief, Defendant Visa USA has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district,

and elsewhere in the United States, by, among other things, methods practiced on various websites (including, without limitation to, visaextras.com, visa.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. Without limitation, when Visa USA and/or Visa USA's customers connect to Visa USA's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Visa USA's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Visa USA provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Visa USA generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Visa USA encrypts data for transmission from the host server to the client. In addition, Visa USA directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Visa USA generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Visa USA decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Visa USA is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

35. Upon information and belief, Defendant Visa Int'l has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various websites (including, without limitation to, visaextras.com, visa.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. Without limitation, when Visa Int'l and/or Visa Int'l's customers connect to Visa Int'l's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Visa Int'l's website, client

computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Visa Int'l provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Visa Int'l generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Visa Int'l encrypts data for transmission from the host server to the client. In addition, Visa Int'l directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Visa Int'l generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Visa Int'l decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Visa Int'l is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

36. Upon information and belief, Defendant AMEX has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the ‘730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various websites (including, without limitation to, americanexpress.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the ‘730 Patent to the injury of TQP. Without limitation, when AMEX and/or AMEX’s customers connect to AMEX’s website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of AMEX’s website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. AMEX provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. AMEX generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. AMEX encrypts data for transmission from the host server to the client. In addition, AMEX directs the client

computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. AMEX generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. AMEX decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant AMEX is thus liable for infringement of the ‘730 Patent pursuant to 35 U.S.C. § 271.

37. Upon information and belief, Defendant AMEX Travel has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the ‘730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various websites (including, without limitation to, americanexpress.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the ‘730 Patent to the injury of TQP. Without limitation, when AMEX Travel and/or AMEX Travel’s customers connect to AMEX Travel’s website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the

host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of AMEX Travel's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. AMEX Travel provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. AMEX Travel generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. AMEX Travel encrypts data for transmission from the host server to the client. In addition, AMEX Travel directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. AMEX Travel generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. AMEX Travel decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant AMEX Travel is thus liable for infringement of the ‘730 Patent pursuant to 35 U.S.C. § 271.

38. Upon information and belief, Defendant MasterCard has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the ‘730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various websites (including, without limitation to, mastercard.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the ‘730 Patent to the injury of TQP. Without limitation, when MasterCard and/or MasterCard’s customers connect to MasterCard’s website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of MasterCard’s website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. MasterCard provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. MasterCard generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new

key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. MasterCard encrypts data for transmission from the host server to the client. In addition, MasterCard directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. MasterCard generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. MasterCard decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant MasterCard is thus liable for infringement of the ‘730 Patent pursuant to 35 U.S.C. § 271.

39. Upon information and belief, Defendant MasterCard Int’l has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the ‘730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various websites (including, without limitation to, mastercard.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the ‘730 Patent to the injury of TQP. Without limitation, when MasterCard Int’l and/or MasterCard Int’l’s customers connect to MasterCard Int’l’s website, a communication link is

established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of MasterCard Int'l's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. MasterCard Int'l provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. MasterCard Int'l generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. MasterCard Int'l encrypts data for transmission from the host server to the client. In addition, MasterCard Int'l directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. MasterCard Int'l generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. MasterCard Int'l decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant MasterCard Int'l is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

40. On information and belief, to the extent any marking was required by 35 U.S.C. § 287, all predecessors in interest to the '730 Patent complied any with such requirements.

41. To the extent that facts learned in discovery show that Defendants' infringement of the '730 patent is or has been willful, Plaintiff reserves the right to request such a finding at time of trial.

42. As a result of these Defendants' infringement of the '730 Patent, Plaintiff has suffered monetary damages in an amount adequate to compensate for Defendants' infringement, but in no event less than a reasonable royalty for the use made of the invention Defendants, together with interest and costs as fixed by the court, and Plaintiff will continue to suffer damages in the future unless Defendants' infringing activities are enjoined by this Court.

43. Unless a permanent injunction is issued enjoining these Defendants and their agents, servants, employees, representatives, affiliates, and all others acting on in active concert therewith from infringing the '730 Patent, Plaintiff will be greatly and irreparably harmed. Alternatively, Plaintiff reserves the right to seek an award of post-judgment royalties if no injunction is entered.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter:

1. A judgment in favor of Plaintiff that Defendants have infringed, directly and

jointly, jointly, and/or indirectly, by way of inducing and/or contributing to the infringement of the '730 Patent, and that such infringement was willful;

2. A permanent injunction enjoining Defendants and their officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in active concert therewith from infringement, inducing the infringement of, or contributing to the infringement of the '730 Patent;

3. A judgment and order requiring Defendants to pay Plaintiff its damages, costs, expenses, and prejudgment and post-judgment interest for Defendants' infringement of the '730 Patent as provided under 35 U.S.C. § 284;

4. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees; and

5. Any and all other relief to which Plaintiff may show itself to be entitled.

DEMAND FOR JURY TRIAL

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

Respectfully submitted,

TQP DEVELOPMENT, LLC

Dated: March 25, 2009

By: /s/ Marc A. Fenster
Marc A. Fenster, CA Bar # 181067
E-mail: mfenster@raklaw.com
RUSS, AUGUST & KABAT
12424 Wilshire Boulevard, 12th Floor
Los Angeles, California 90025
Telephone: 310/826-7474
Facsimile: 310/826-6991

Harold Kip Glasscock, Jr., TX Bar # 08011000
LEAD COUNSEL
E-mail: kipglasscock@hotmail.com
KIP GLASSCOCK, P.C.
550 Fannin Suite 1350
Beaumont, Texas 77701
Telephone: 409/833-8822
Facsimile: 409/838-4666

ATTORNEYS FOR PLAINTIFF
TQP DEVELOPMENT, LLC