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

TQP DEVELOPMENT, LLC, Plaintiff, **v.** **1. DELL INC.;** **2. UNITED CONTINENTAL HOLDINGS, INC.;** **3. UNITED AIR LINES, INC.;** **4. LOWE'S COMPANIES, INC.;** **5. LOWE'S HOME CENTERS, INC.;** **6. LOWE'S HIW, INC.;** **7. DEUTSCHE TELEKOM AG;** **8. T-MOBILE USA, INC.;** **9. DISCOVER FINANCIAL SERVICES;** **10. HEWLETT-PACKARD COMPANY;** **11. HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.;** **12. CHEVRON CORPORATION;** **13. CHEVRON U.S.A. INC.;** **14. RESEARCH IN MOTION LIMITED;** **15. RESEARCH IN MOTION CORPORATION; AND** **16. COSTCO WHOLESALE CORPORATION,** Defendants.	**Civil Action No. 2:10-cv-446** **JURY TRIAL DEMANDED**

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

This is an action for patent infringement in which TQP Development, LLC ("TQP") makes the following allegations against Dell Inc.; United Continental Holdings, Inc.; United Air Lines, Inc.; Lowe's Companies, Inc.; Lowe's Home Centers, Inc.; Lowe's HIW, Inc.; Deutsche Telekom AG; T-Mobile USA, Inc.; Discover Financial Services; Hewlett-Packard Company; Hewlett-Packard Development Company, L.P.; Chevron Corporation; Chevron U.S.A. Inc.;

Research in Motion Limited; Research in Motion Corporation; and Costco Wholesale Corporation (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 Street, Marshall, Texas 75670.

2. On information and belief, Defendant Dell Inc. ("Dell") is a Delaware corporation with its principal place of business at One Dell Way, Round Rock, Texas 78682. Dell has appointed Corporation Service Company, 2711 Centerville Road, Suite 400, Wilmington, Delaware 19808 as its agent for service of process.

3. On information and belief, Defendant United Continental Holdings, Inc. ("United Continental") is a Delaware corporation with its principal place of business at 77 W. Wacker Drive, Chicago, Illinois 60601. United Continental has appointed The Prentice-Hall Corporation System, Inc., Centerville Road, Suite 400, Wilmington, Delaware 19808 as its agent for service of process.

4. On information and belief, Defendant United Air Lines, Inc. ("United Air") is a Delaware corporation with its principal place of business at 77 W. Wacker Drive, Chicago, Illinois 60601. United Air has appointed The Prentice-Hall Corporation System, Inc., 2711 Centerville Road, Suite 400, Wilmington, Delaware 19808 as its agent for service of process.

5. On information and belief, Defendant Lowe's Companies, Inc. ("Lowe's Companies") is a North Carolina corporation with its principal place of business at 1000 Lowe's Boulevard, Mooresville, North Carolina 28117. Lowe's Companies has appointed Corporation Service Company, 327 Hillsborough Street, Raleigh, North Carolina 27603 as its agent for service of process.

6. On information and belief, Defendant Lowe's Home Centers, Inc. ("Lowe's Home") is a North Carolina corporation with its principal place of business at 1605 Curtis Bridge Rd., Wilkesboro, North Carolina 28697. Lowe's Home has appointed Corporation Service Company, 327 Hillsborough Street, Raleigh, North Carolina 27603 as its agent for service of process.

7. On information and belief, Defendant Lowe's HIW, Inc. ("Lowe's HIW") is a Washington corporation with its principal place of business at 101 Andover Park E., Tukwila, Washington 98188. Lowe's HIW has appointed Corporation Service Company, 300 Deschutes Way SW, STE 304, Tumwater, Washington 98501 as its agent for service of process.

8. On information and belief, Defendant Deutsche Telekom AG ("Deutsche Telekom") is a German corporation with its principal place of business at Friedrich-Ebert-Allee 140, Bonn, 53113, Germany. Deutsche Telekom may be served at Friedrich-Ebert-Allee 140, Bonn, 53113, Germany via an officer, a managing or general agent, or any other agent authorized by appointment or by law to receive service of process.

9. On information and belief, Defendant T-Mobile USA, Inc. ("T-Mobile") is a Washington corporation with its principal place of business at 12920 SE 38th St., Bellevue, Washington 98006. T-Mobile has appointed Corporation Service Company, 300 Deschutes Way SW, STE 304, Tumwater, Washington 98501 as its agent for service of process.

10. On information and belief, Defendant Discover Financial Services ("Discover") is a Delaware corporation with its principal place of business at 2500 Lake Cook Road, Riverwoods, Illinois 60015. Discover has appointed The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, Delaware 19801 as its agent for service of process.

11. On information and belief, Defendant Hewlett-Packard Company ("HP") is a Delaware corporation with its principal place of business at 3000 Hanover Street, Palo Alto, California 94304. HP has appointed The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, Delaware 19801 as its agent for service of process.

12. On information and belief, Defendant Hewlett-Packard Development Company, L.P. ("HP Development") is a Texas corporation with its principal place of business at 20555 State Highway 249, Houston, Texas 77070. HP Development has appointed CT Corp. System, 350 N. St. Paul St. Ste. 2900, Dallas, Texas 75201 as its agent for service of process.

13. On information and belief, Defendant Chevron Corporation ("Chevron") is a Delaware corporation with its principal place of business at 6001 Bollinger Canyon Road, San Ramon, California 94583. Chevron has appointed The Prentice-Hall Corporation System, Inc., 2711 Centerville Road Suite 400, Wilmington, Delaware 19808 as its agent for service of process.

14. On information and belief, Defendant Chevron U.S.A. Inc. ("Chevron USA") is a Pennsylvania corporation with its principal place of business at 6001 Bollinger Canyon Road, San Ramon, California 94583. Chevron USA has appointed The Prentice-Hall Corporation System, Inc., 2730 Gateway Oaks Dr. Ste. 100, Sacramento, California 95833 as its agent for service of process.

15. On information and belief, Research in Motion Limited ("RIM") is a Canada corporation with its principal place of business at 295 Phillip Street, Waterloo, Ontario N2L 3W8, Canada. Research in Motion Limited may be served at 295 Phillip Street, Waterloo, Ontario N2L 3W8, Canada via an officer, a managing or general agent, or any other agent authorized by appointment or by law to receive service of process.

16. On information and belief, Defendant Research in Motion Corporation ("RIM Corporation") is a Delaware corporation with its principal place of business at 122 W. John Carpenter Fwy., Irving, TX 75039. Research in Motion Corporation has appointed The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801 as its agent for service of process.

17. On information and belief, Defendant Costco Wholesale Corporation ("Costco") is a Washington corporation with its principal place of business at 999 Lake Drive, Issaquah, Washington 98027. Costco has appointed John Sullivan, 999 Lake Dr., Issaquah, Washington 98027 as its agent for service of process.

JURISDICTION AND VENUE

18. 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).

19. 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.

20. 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 Statue, 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

21. 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.

22. Upon information and belief, Defendant Dell has been and now is infringing the '402 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Dell websites (including, without limitation to, ecomm.dell.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. For example, when Dell and/or Dell's customers connect to Dell'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 Dell'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. Dell 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. Dell 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. Dell encrypts data for transmission from the host server to the client. In addition, Dell directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Dell 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. Dell 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. By virtue of performing each step of the claimed method, Defendant Dell is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Dell is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Dell is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

23. Upon information and belief, Defendant United Continental has been and now is infringing the '402 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various United Continental websites

(including, without limitation to, www.ua2go.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. For example, when United Continental and/or United Continental's customers connect to United Continental'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 United Continental'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. United Continental 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. United Continental 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. United Continental encrypts data for transmission from the host server to the client. In addition, United Continental directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. United Continental 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. United Continental 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. By virtue of performing each step of the claimed method, Defendant United Continental is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant United Continental is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant United Continental is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

24. Upon information and belief, Defendant United Air has been and now is infringing the '402 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various United Air websites (including, without limitation to, www.ua2go.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. For example, when United Air and/or United Air's customers connect to United Air'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 United Air'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. United Air 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. United Air 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. United Air encrypts data for transmission from the host server to the client. In addition, United Air directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. United Air 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. United Air 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. By virtue of performing each step of the claimed method, Defendant United Air is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant United Air is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant United Air is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

25. Upon information and belief, Defendant Lowe's Companies has been and now is infringing the '402 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Lowe's Companies websites (including, without limitation to, www.lowes.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. For example, when Lowe's Companies and/or Lowe's Companies' customers connect to Lowe's Companies' 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 Lowe'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. Lowe's 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. Lowe's Companies 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. Lowe's Companies encrypts data for transmission from the host server to the client. In addition, Lowe's Companies directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Lowe's Companies 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. Lowe's Companies 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. By virtue of performing each step of the claimed method, Defendant Lowe's Companies is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Lowe's Companies is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Lowe's Companies is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

26. Upon information and belief, Defendant Lowe's Home has been and now is infringing the '402 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Lowe's Home websites (including, without limitation to, www.lowes.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. For example, when Lowe's Home and/or Lowe's Home's customers connect to Lowe's Home'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 Lowe's Home'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. Lowe's Home 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. Lowe's Home 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. Lowe's Home encrypts data for transmission from the host server to the client. In addition, Lowe's Home directs the client computer to encrypt data comprising information sent

from the client to the host server before it is transmitted over the link. Lowe's Home 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. Lowe's Home 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. By virtue of performing each step of the claimed method, Defendant Lowe's Home is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Lowe's Home is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Lowe's Home is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

27. Upon information and belief, Defendant Lowe's HIW has been and now is infringing the '402 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Lowe's HIW websites (including, without limitation to, www.lowes.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. For example, when Lowe's HIW and/or Lowe's HIW's customers connect to Lowe's HIW'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 Lowe's HIW'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. Lowe's HIW 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. Lowe's HIW 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. Lowe's HIW encrypts data for transmission from the host server to the client. In addition, Lowe's HIW directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Lowe's HIW 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. Lowe's HIW 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. By virtue of performing each step of the claimed method, Defendant Lowe's HIW is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Lowe's HIW is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Lowe's HIW is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

28. Upon information and belief, Defendant Deutsche Telekom has been and now is infringing the '402 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Deutsche Telekom websites (including, without limitation to, my.t-mobile.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. For example, when Deutsche Telekom and/or Deutsche Telekom's customers connect to Deutsche Telekom'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 Deutsche Telekom'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. Deutsche Telekom 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. Deutsche Telekom 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. Deutsche Telekom encrypts data for transmission from the host server to the client. In addition, Deutsche Telekom directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Deutsche Telekom 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. Deutsche Telekom 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. By virtue of performing each step of the claimed method, Defendant Deutsche Telekom is directly infringing the ‘730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Deutsche Telekom is directly infringing,

literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Deutsche Telekom is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

29. Upon information and belief, Defendant T-Mobile has been and now is infringing the '402 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various T-Mobile websites (including, without limitation to, my.t-mobile.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. For example, when T-Mobile and/or T-Mobile's customers connect to T-Mobile'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 T-Mobile'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. T-Mobile 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. T-Mobile 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. T-Mobile encrypts data for transmission from the host server to the client. In addition, T-Mobile directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. T-Mobile 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. T-Mobile 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. By virtue of performing each step of the claimed method, Defendant T-Mobile is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant T-Mobile is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant T-Mobile is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

30. Upon information and belief, Defendant Discover has been and now is infringing the '402 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Discover websites (including, without limitation to, www.discovercard.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. For example, when Discover and/or Discover's customers connect to Discover'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 Discover'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. Discover 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. Discover 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. Discover encrypts data for transmission from the host server to the client. In addition, Discover directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Discover 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. Discover 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. By virtue of performing each step of the claimed method, Defendant Discover is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Discover is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Discover is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

31. Upon information and belief, Defendant HP has been and now is infringing the '402 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various HP websites (including, without limitation to, www.shopping.hp.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. For example, when HP and/or HP's customers connect to HP'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 HP'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. HP 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. HP 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. HP encrypts data for transmission from the host server to the client. In addition, HP directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. HP 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. HP 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. By virtue of performing each step of the claimed method, Defendant HP is directly infringing the ‘730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant HP is directly infringing, literally infringing, and/or infringing the ‘730 Patent under

the doctrine of equivalents. Defendant HP is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. § 271.

32. Upon information and belief, Defendant HP Development has been and now is infringing the ‘402 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various HP Development websites (including, without limitation to, www.shopping.hp.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. For example, when HP Development and/or HP Development’s customers connect to HP Development’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 HP Development’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. HP Development 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. HP Development 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. HP Development encrypts data for transmission from the host server to the client. In addition, HP Development directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. HP Development 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. HP Development 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. By virtue of performing each step of the claimed method, Defendant HP Development is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant HP Development is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant HP Development is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

33. Upon information and belief, Defendant Chevron has been and now is infringing the '402 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Chevron websites (including, without limitation to, www.chevrontexacocards.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. For example, when Chevron and/or Chevron's customers connect to Chevron'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 Chevron'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. Chevron 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. Chevron 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. Chevron encrypts data for transmission from the host server to the client. In addition, Chevron directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Chevron 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. Chevron 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. By virtue of performing each step of the claimed method, Defendant Chevron is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Chevron is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Chevron is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

34. Upon information and belief, Defendant Chevron USA has been and now is infringing the '402 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Chevron USA websites (including, without limitation to, www.chevrontexacocards.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. For example, when Chevron USA and/or Chevron USA's customers connect to Chevron 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 Chevron 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. Chevron 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. Chevron 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. Chevron USA encrypts data for transmission from the host server to the client. In addition, Chevron 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. Chevron 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. Chevron 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. By virtue of performing each step of the claimed method, Defendant Chevron USA is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to

perform the remaining steps, Defendant Chevron USA is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Chevron USA is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

35. Upon information and belief, Defendant RIM has been and now is infringing the '402 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various RIM websites (including, without limitation to, www.blackberry.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. For example, when RIM and/or RIM's customers connect to RIM'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 RIM'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. RIM 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. RIM 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. RIM encrypts data for transmission from the host server to the client. In addition, RIM directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. RIM 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. RIM 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. By virtue of performing each step of the claimed method, Defendant RIM is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant RIM is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant RIM is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

36. Upon information and belief, Defendant RIM Corporation has been and now is infringing the '402 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various RIM Corporation websites (including, without limitation to, www.blackberry.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. For example, when RIM Corporation and/or RIM

Corporation's customers connect to RIM Corporation'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 RIM Corporation'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. RIM Corporation 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. RIM Corporation 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. RIM Corporation encrypts data for transmission from the host server to the client. In addition, RIM Corporation directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. RIM Corporation 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. RIM Corporation 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. By virtue of performing each step of the claimed method, Defendant RIM Corporation is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant RIM Corporation is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant RIM Corporation is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

37. Upon information and belief, Defendant Costco has been and now is infringing the '402 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Costco websites (including, without limitation to, www.costco.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. For example, when Costco and/or Costco's customers connect to Costco'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 Costco'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. Costco 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. Costco 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. Costco encrypts data for transmission from the host server to the client. In addition, Costco directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Costco 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. Costco 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. By virtue of performing each step of the claimed method, Defendant Costco is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Costco is directly infringing, literally

infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Costco is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

38. 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 with any such requirements.

39. 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 the time of trial.

40. As a result of these Defendants' infringement of the '730 Patent, Plaintiff has suffered monetary damages and is entitled to a money judgment 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 by 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.

41. 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.

PRAYER FOR RELIEF

Wherefore, Plaintiff respectfully requests that this Court enter:

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

Dated: October 20, 2010

Respectfully submitted,

By: /s/ *Marc A. Fenster*
Marc A. Fenster, CA Bar # 181067
E-mail: mfenster@raklaw.com
Alex C. Giza, CA Bar No. 212327
Email: agiza@raklaw.com
Adam S. Hoffman, CA Bar No. 218740
Email: ahoffman@raklaw.com
Andrew Weiss, CA Bar No. 232974
Email: aweiss@raklaw.com
RUSS, AUGUST & KABAT
12424 Wilshire Boulevard, 12th Floor
Los Angeles, California 90025
Telephone: 310/826-7474
Facsimile: 310/826-6991

Hao Ni, TX Bar No. 24047205
E-mail: hni@nilawfirm.com
Ni Law Firm, PLLC
3102 Maple Ave. Suite 400
Dallas, TX 75201

Telephone: 214/800-2208
Facsimile: 214/880-2209

Andrew Wesley Spangler
E-mail: spangler@spanglerlawpc.com
SPANGLER LAW P.C.
208 N. Green Street, Suite 300
Longview, Texas 75601
Telephone: 903/753-9300
Facsimile: 903/553-0403

ATTORNEYS FOR PLAINTIFF
TQP DEVELOPMENT, LLC