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

TQP DEVELOPMENT, LLC, Plaintiff **v.** **(1) BANK OF NEW YORK MELLON CORPORATION;** **(2) THE ALLSTATE INSURANCE COMPANY;** **(3) WALGREEN COMPANY;** **(4) DELTA AIR LINES, INC.;** **(5) UBS FINANCIAL SERVICES INC.;** **(6) UBS AG;** **(7) WESTERN UNION FINANCIAL SERVICES, INC.;** **(8) TIME WARNER CABLE INC.;** **(9) TIME WARNER INC.** **(10) BIGMACHINES INC.;** **(11) TRANSAMERICA LIFE INSURANCE COMPANY; and** **(12) THE LINCOLN NATIONAL LIFE INSURANCE COMPANY** Defendants.		**Civil Action No. 2:10-CV-085** **JURY TRIAL DEMANDED**

SECOND AMENDED COMPLAINT FOR PATENT INFRINGEMENT

This is an action for patent infringement in which TQP Development, LLC ("TQP") makes the following allegations against Bank of New York Mellon Corporation, The Allstate Insurance Company, Walgreen Company, Delta Air Lines, Inc., UBS Financial Services Inc., UBS AG, Inc, Western Union Financial Services, Inc., Time Warner Cable Inc., Time Warner Inc., BigMachines Inc., Transamerica Life Insurance Company, and The Lincoln National Life Insurance Company (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 Bank of New York Mellon Corporation ("BNY Mellon") is a Delaware corporation with its principal place of business at One Wall Street, New York, NY 12806. BNY Mellon has appointed The Corporation Trust Company, Corporation Trust Center, 1209 Orange St., Wilmington, DE 19801, as its agent for service of process.

3. On information and belief, Defendant The Allstate Insurance Company ("Allstate") is an Illinois corporation with its principal place of business at 2775 Sanders Rd., Northbrook, IL 60062. Allstate has appointed The Corporation Trust Company, 400 Cornerstone Dr., 240, Williston, VT 05495-4019, as its agent for service of process.

4. On information and belief, Defendant Walgreen Company ("Walgreen") is an Illinois corporation with its principal place of business at 200 Wilmot Rd., Deerfield, IL 60015. Walgreen has appointed Illinois Corporation Service Co., 801 Adlai Stevenson Drive, Springfield, IL 62703, as its agent for service of process.

5. On information and belief, Defendant Delta Air Lines, Inc. ("Delta") is a Delaware corporation with its principal place of business at Hartsfield Atlanta International Air Port, 1030 Delta Blvd, Atlanta, GA 30354-1989. Delta has appointed Corporation Service Co., 2711 Centerville Road, Suite 400, Wilmington, DE 19808, as its agent for service of process.

6. On information and belief, UBS Financial Services ("UBS") is a Delaware corporation with its U.S. principal place of business at 1285 Avenue of the Americas, New York, NY 10019. UBS has appointed, Corporation Service Company, 2711 Centerville Rd. Suite 400, Wilmington, DE 19808, as its agent for service of process.

7. On information and belief, UBS AG, ("UBS AG") is a Swiss corporation with its U.S. principal place of business at 1285 Avenue of the Americas, New York, NY 10019. UBS AG has appointed Corporation Service Company dba CSC-Lawyers Incorporating Service Company, l701 Brazos, Suite 1050, Austin, TX 78701, as its agent for service of process.

8. On information and belief, Western Union Financial Services, Inc. ("Western Union") is a Colorado corporation with its principal place of business at 6200 S. Quebec St, Suite 450, Greenwood Village, CO 80111. Western Union has appointed Corporation Service Co., 211 E. 7th Street, Suite 620, Austin, TX 78701, as its agent for service of process.

9. On information and belief, Time Warner Cable Inc. ("TWC") is a Delaware corporation with its principal place of business at 60 Columbus Circle, New York, NY 10023. TWC has appointed Corporation Trust Co., Corporation Trust Center, 1209 Orange St., Wilmington, DE 19801, as its agent for service of process.

10. On information and belief, Time Warner Inc. ("TW") is a Pennsylvania corporation with its principal place of business at One TWC Center, New York, NY 10019. TW has appointed Corporation Trust Co., Corporation Trust Center, 1209 Orange St., Wilmington, DE 19801, as its agent for service of process.

11. On information and belief, BigMachines, Inc. ("BigMachines") is a Delaware corporation with its principal place of business at 570 Lake Cook Rd, Ste 126, Deerfield, IL 60015-4953. BigMachines has appointed Corporation Service Co., 2711 Centerville Road, Suite 400 Wilmington, DE 19808, as its agent for service of process.

12. On information and belief, Transamerica Life Insurance Corporation ("Transamerica") is an Iowa corporation with its principal place of business at 4333 Edgewood Rd NE, Cedar Rapids, IA 52499. Transamerica has appointed Craig Vermie, 4333 Edgewood Rd NE, Cedar Rapids IA 52408, as its agent for service of process.

13. On information and belief, The Lincoln National Life Insurance Company ("Lincoln") is an Indiana corporation with its principal place of business at 1300 South Clinton St., Fort Wayne, IN, 46802. Lincoln has appointed The Prentice-Hall Corporation System, Inc. 251 E Ohio St, Ste 500, Indianapolis, IN 46204, as its agent for service of process.

JURISDICTION AND VENUE

14. 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).

15. 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.

16. 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

17. 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.

18. Upon information and belief, Defendant BNY Mellon has been and now is directly and jointly 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 Stated, by, among other things, methods practiced on various websites (including, without limitation to, gm.bankofny.com, clients.bnyconvergext.com and bnymellon.ebanking-services.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 BNY Mellon and/or BNY Mellon's customers connect to BNY Mellon'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 BNY Mellon'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. BNY Mellon 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. BNY Mellon 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. BNY Mellon encrypts data for transmission from the host server to the client. In addition, BNY Mellon directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. BNY Mellon 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. BNY Mellon 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 BNY Mellon 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 BNY Mellon is directly infringing, literally infringing, and/or infringing the ‘730 Patent under the doctrine of equivalents. Defendant BNY Mellon is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. §271

19. Upon information and belief, Defendant Allstate has been and now is directly and jointly 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, customercare.allstate.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 Allstate and/or Allstate’s customers connect to Allstate’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 Allstate’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. Allstate 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. Allstate 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. Allstate encrypts data for transmission from the host server to the client. In addition, Allstate directs the client

computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Allstate 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. Allstate 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 Allstate is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. § 271.

20. Upon information and belief, Defendant Walgreen has been and now is directly and jointly 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, www.walgreens.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 Walgreen and/or Walgreen’s customers connect to Walgreen’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 Walgreen'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. Walgreen 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. Walgreen 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. Walgreen encrypts data for transmission from the host server to the client. In addition, Walgreen directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Walgreen 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. Walgreen 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 Walgreen is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. § 271.

21. Upon information and belief, Defendant Target has been and now is directly and jointly 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, www.target.com and rcam.target.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 Target and/or Targets’ customers connect to Target’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 Target’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. Target 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. Target 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. Target encrypts data for transmission from the host server to the client. In addition, Target directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Target 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. Target 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 Target is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. § 271.

22. Upon information and belief, Defendant Delta has been and now is directly and jointly 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, www.delta.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 Delta and/or Delta’s customers connect to Delta’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 Delta'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. Delta 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. Delta 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. Delta encrypts data for transmission from the host server to the client. In addition, Delta directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Delta 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. Delta 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 Delta is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. § 271.

23. Upon information and belief, Defendant UBS has been and now is directly and jointly 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, onlineservices.ubs.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 UBS and/or UBS’s customers connect to UBS’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 UBS’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. UBS 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. UBS 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. UBS encrypts data for transmission from the host server to the client. In addition, UBS directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. UBS 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. UBS 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 UBS is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. § 271.

24. Upon information and belief, Defendant UBS AG has been and now is directly and jointly 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, globalam-us.ubs.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 UBS AG and/or UBS AG’s customers connect to UBS AG’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 UBS AG'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. UBS AG 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. UBS AG 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. UBS AG encrypts data for transmission from the host server to the client. In addition, UBS AG directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. UBS AG 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. UBS AG 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 UBS AG is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. § 271.

25. Upon information and belief, Defendant Western Union has been and now is directly and jointly 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, wumt.westernunion.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 Western Union and/or Western Union’s customers connect to Western Union’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 Western Union’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. Western Union 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. Western Union 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. Western Union encrypts data for transmission from the host server to the client. In addition, Western Union directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Western Union 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. Western Union 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 Western Union is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. § 271.

26. Upon information and belief, Defendant TWC has been and now is directly and jointly 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, twlax.convergentcare.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 TWC and/or TWC’s customers connect to TWC’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 TWC’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. TWC 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. TWC 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. TWC encrypts data for transmission from the host server to the client. In addition, TWC directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. TWC 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. TWC 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 TWC is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. § 271.

27. Upon information and belief, Defendant TW has been and now is directly and jointly 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, subs.timeinc.com, cartoonnetworkshop.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 TW and/or TW’s customers connect to TW’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 TW’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 implement the claimed encryption algorithm under the direction of the host server. TW 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. TW

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. TW encrypts data for transmission from the host server to the client. In addition, TW directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. TW 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. TW 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 TW is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. § 271.

28. Upon information and belief, Defendant BigMachines has been and now is directly and jointly 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, shoretel.bigmachines.com and

enterasys.bigmachines.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 BigMachines and/or BigMachines’ customers connect to BigMachines’ 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 BigMachines’ 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. BigMachines 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. BigMachines 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. BigMachines encrypts data for transmission from the host server to the client. In addition, BigMachines directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. BigMachines 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. BigMachines 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 BigMachines is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. § 271.

29. Upon information and belief, Defendant Transamerica has been and now is directly and jointly 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, afp.transamerica.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 Transamerica and/or Transamerica’s customers connect to Transamerica’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 Transamerica’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. Transamerica 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. Transamerica 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. Transamerica encrypts data for transmission from the host server to the client. In addition, Transamerica directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Transamerica 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. Transamerica 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 Transamerica is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. § 271.

30. Upon information and belief, Defendant Lincoln has been and now is directly and jointly 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, www.lfg.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 Lincoln and/or Lincoln’s customers connect to Lincoln’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 Lincoln’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. Lincoln 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. Lincoln 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. Lincoln encrypts data for transmission from the host server to the client. In addition, Lincoln directs the client

computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Lincoln 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. Lincoln 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 Lincoln is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. § 271.

31. 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.

32. 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.

33. 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.

34. 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: May 10, 2010

Respectfully submitted,

By: /s/ *Hao Ni*

Andrew Wesley Spangler
Spangler Law PC
208 N. Green St.
Suite 300
Longview, TX 75601
903-753-9300
Fax: 903-553-0403
Email: spangler@spanglerlawpc.com

Hao Ni
Texas Bar No. 24047205
Ni Law Firm, PLLC
3102 Maple Ave. Suite 400
Dallas, TX 75201
Telephone: (214) 800-2208
Fax: (214) 880-2209
E-mail: hni@nilawfirm.com

Marc A. Fenster, CA Bar No. 181067
Andrew D. Weiss, CA Bar No. 232974
E-mail: mfenster@raklaw.com
E-mail: aweiss@raklaw.com
RUSS, AUGUST & KABAT
12424 Wilshire Boulevard 12th Floor
Los Angeles, California 90025
Telephone: 310/826-7474
Facsimile: 310/826-6991

John Marcus Bustamante
State Bar No. 24040618
jmb@bustamantelegal.com
Bustamante PC
54 Rainey St. No. 721
Austin, TX 78701
Telephone: 512-940-3753
Facsimile: 512-551-3773

Patrick R. Anderson,
MI Bar No. 24059490
E-mail: patrick@prapllc.com

Patrick R. Anderson PLLC
4225 Miller Rd., Bldg. B-p, Suite 358
Flint, MI 88597
Telephone: 517-303-4806
Fax: 248-928-9239
Attorneys for Plaintiff
TQP DEVELOPMENT, LLC

CERTIFICATE OF SERVICE

I hereby certify that the counsel of record who are deemed to have consented to electronic service are being served today with a copy of this document via the Court's CM/ECF system per Local Rule CV-5(a)(3). Any other counsel of record will be served by electronic mail, facsimile transmission and/or first class mail on this same date.

May 10, 2010 /s/ Hao Ni
Hao Ni