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

TQP DEVELOPMENT, LLC, Plaintiff, **v.** **1-800-FLOWERS.COM, INC. et al.,** Defendants	**C. A. No. 2:11-cv-248-JRG-RSP** **JURY TRIAL DEMANDED**

SUPPLEMENTAL COMPLAINT FOR PATENT INFRINGEMENT

TQP Development, LLC ("TQP") makes the following supplemental allegations against Alticor, Inc. ("Alticor"), Amway Corp. ("Amway"), HSN, Inc. ("HSN"), Newegg, Inc. ("Newegg"), and QVC, Inc. ("QVC") (collectively the "Defendants").

PARTIES

1. Paragraphs 1, 3, 4, 6, 8, and 9 of TQP's Original Complaint for Patent Infringement ("Complaint") (Dkt. No. 1) are adopted here pursuant to Fed. R. Civ. P. 10(b) and 10(c).

JURISDICTION AND VENUE

2. Paragraphs 12 through 14 of TQP's Complaint are adopted here pursuant to Fed. R. Civ. P. 10(b) and 10(c).

COUNT I

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

3. Paragraph 15 of TQP's Complaint is adopted here pursuant to Fed. R. Civ. P. 10(b) and 10(c).

4. Paragraph 17 of TQP's Complaint is adopted here pursuant to Fed. R. Civ. P. 10(b) and 10(c). Additionally, and in the alternative, upon information and belief, Defendant Alticor has induced infringement of the '730 patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, performing certain steps of the methods claimed by the '730 patent, and advising, encouraging, or otherwise inducing others to perform the remaining steps claimed by the '730 Patent to the injury of TQP. For example, Alticor has configured the equipment that hosts its secure websites ("Host Server") (including, without limitation to, www.amway.com), or caused the Host Server to be configured, to require use of the SSL and/or TLS encryption protocols. An SSL/TLS handshake takes place when, for example, an Alticor customer, potential customer, or client connects to a secure Alticor website with a computer or mobile device ("Client Computer"). The Host Server of Alticor determines which cipher is used for encryption and decryption at the transmitter and receiver of the Host Server and the Client Computer during the SSL/TLS handshake. A communication link covered by one or more claims of the '730 patent was established between the Host Server and the Client Computer when the Host Server determined that the RC4 encryption algorithm would be used during the SSL/TLS handshake. Data transmitted over the communication link (both from the Client Computer to the Host Server, and from the Host Server to the Client Computer) comprises a sequence of blocks, and was transmitted as packets in a sequence over the communication link. The Client

Computer and the Host Server automatically encrypted and decrypted the data transmitted over the communication link pursuant to the method steps claimed by the ‘730 patent. The Client Computer and the Host Server automatically provided a seed value to the transmitter and receiver that were used to encrypt and decrypt the data transmitted over the communication link. A first sequence of pseudo-random key values was automatically generated at the transmitter (whichever of the Host Server or Client Computer was sending the encrypted information) to encrypt the data based on said seed values, 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. Alticor has encrypted data and transmitted data from the Host Server to the Client Computer over said link. In addition, by using its Host Server to determine that the RC4 encryption algorithm would be used, Alticor has induced users of the Client Computer to automatically encrypt and transmit data over said link to the Host Server. Alticor has generated, and, by using its Host Server to determine that the RC4 encryption algorithm would be used, has caused the Client Computer to automatically generate a second sequence of pseudo-random key values 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. Alticor has decrypted data sent from the Client Computer over said link in order to use the data, and, by using its Host Server to determine that the RC4 encryption algorithm would be used, has caused the Client Computer to automatically decrypt data transmitted from the Host Server over said link in order to provide a useable display to the user of the Client Computer. Since at least May 6, 2011, when TQP's Complaint was filed, Alticor has had knowledge of the '730 patent and, by continuing the actions described above, has had the specific intent to induce infringement of the '730 patent pursuant to 35 U.S.C. § 271(b).

5. Paragraph 18 of TQP's Complaint is adopted here pursuant to Fed. R. Civ. P. 10(b) and 10(c). Additionally, and in the alternative, upon information and belief, Defendant Amway has induced infringement of the '730 patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, performing certain steps of the methods claimed by the '730 patent, and advising, encouraging, or otherwise inducing others to perform the remaining steps claimed by the '730 Patent to the injury of TQP. For example, Amway has configured the equipment that hosts its secure websites ("Host Server") (including, without limitation to, www.amway.com), or caused the Host Server to be configured, to require use of the SSL and/or TLS encryption protocols. An SSL/TLS handshake takes place when, for example, an Amway customer, potential customer, or client connects to a secure Amway website with a computer or mobile device ("Client Computer"). The Host Server of Amway determines which cipher is used for encryption and decryption at the transmitter and receiver of the Host Server and Client Computer during the SSL/TLS handshake. A communication link covered by one or more claims of the '730 patent was established between the Host Server and the Client Computer when the Host Server determined that the RC4 encryption algorithm would be used during the SSL/TLS handshake. Data transmitted over the communication link (both from the Client Computer to the Host Server, and from the Host Server to the Client Computer) comprises a sequence of blocks,

and was transmitted as packets in a sequence over the communication link. The Client Computer and the Host Server automatically encrypted and decrypted the data transmitted over the communication link pursuant to the method steps claimed by the ‘730 patent. The Client Computer and the Host Server automatically provided a seed value to the transmitter and receiver that were used to encrypt and decrypt the data transmitted over the communication link. A first sequence of pseudo-random key values was automatically generated at the transmitter (whichever of the Host Server or Client Computer was sending the encrypted information) to encrypt the data based on said seed values, 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. Amway has encrypted data and transmitted data from the Host Server to the Client Computer over said link. In addition, by using its Host Server to determine that the RC4 encryption algorithm would be used, Amway has induced users of the Client Computer to encrypt and transmit data over said link to the Host Server. Amway has generated, and, by using its Host Server to determine that the RC4 encryption algorithm would be used, has caused the Client Computer to automatically generate a second sequence of pseudo-random key values 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. Amway has decrypted data sent from the Client Computer over said link in order to use the data, and, by using its Host Server to determine that the RC4 encryption algorithm would be used, has caused the

Client Computer to automatically decrypt data transmitted from the Host Server over said link in order to provide a useable display to the user of the Client Computer. Since at least May 6, 2011, when TQP's Complaint was filed, Amway has had knowledge of the '730 patent and, by continuing the actions described above, has had the specific intent to induce infringement of the '730 patent pursuant to 35 U.S.C. § 271(b).

6. Paragraph 20 of TQP's Complaint is adopted here pursuant to Fed. R. Civ. P. 10(b) and 10(c). Additionally, and in the alternative, upon information and belief, Defendant HSN has induced infringement of the '730 patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, performing certain steps of the methods claimed by the '730 patent, and advising, encouraging, or otherwise inducing others to perform the remaining steps claimed by the '730 Patent to the injury of TQP. For example, HSN has configured the equipment that hosts its secure websites ("Host Server") (including, without limitation to, www.hsn.com), or caused the Host Server to be configured, to require use of the SSL and/or TLS encryption protocols. An SSL/TLS handshake takes place when, for example, an HSN customer, potential customer, or client connects to a secure HSN website with a computer or mobile device ("Client Computer"). The Host Server of HSN determines which cipher is used for encryption and decryption at the transmitter and receiver of the Host Server and the Client Computer during the SSL/TLS handshake. A communication link covered by one or more claims of the '730 patent was established between the Host Server and the Client Computer when the Host Server determined that the RC4 encryption algorithm would be used during the SSL/TLS handshake. Data transmitted over the communication link (both from the Client Computer to the Host Server, and from the Host Server to the Client Computer) comprises a sequence of blocks,

and was transmitted as packets in a sequence over the communication link. The Client Computer and the Host Server automatically encrypted and decrypted the data transmitted over the communication link pursuant to the method steps claimed by the ‘730 patent. The Client Computer and the Host Server automatically provided a seed value to the transmitter and receiver that were used to encrypt and decrypt the data transmitted over the communication link. A first sequence of pseudo-random key values was automatically generated at the transmitter (whichever of the Host Server or Client Computer was sending the encrypted information) to encrypt the data based on said seed values, 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. HSN has encrypted data and transmitted data from the Host Server to the Client Computer over said link. In addition, by using its Host Server to determine that the RC4 encryption algorithm would be used, HSN has induced users of the Client Computer to encrypt and transmit data over said link to the Host Server. HSN has generated, and, by using its Host Server to determine that the RC4 encryption algorithm would be used, has caused the Client Computer to automatically generate a second sequence of pseudo-random key values 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. HSN has decrypted data sent from the Client Computer over said link in order to use the data, and, by using its Host Server to determine that the RC4 encryption algorithm would be used, has caused the Client

Computer to automatically decrypt data transmitted from the Host Server over said link in order to provide a useable display to the user of the Client Computer. Since at least May 6, 2011, when TQP's Complaint was filed, HSN has had knowledge of the '730 patent and, by continuing the actions described above, has had the specific intent to induce infringement of the '730 patent pursuant to 35 U.S.C. § 271(b).

7. Paragraph 22 of TQP's Complaint is adopted here pursuant to Fed. R. Civ. P. 10(b) and 10(c). Additionally, and in the alternative, upon information and belief, Defendant Newegg has induced infringement of the '730 patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, performing certain steps of the methods claimed by the '730 patent, and advising, encouraging, or otherwise inducing others to perform the remaining steps claimed by the '730 Patent to the injury of TQP. For example, Newegg has configured the equipment that hosts its secure websites ("Host Server") (including, without limitation to, secure.newegg.com), or caused the Host Server to be configured, to require use of the SSL and/or TLS encryption protocols. An SSL/TLS handshake takes place when, for example, a Newegg customer, potential customer, or client connects to a secure Newegg website with a computer or mobile device ("Client Computer"). The Host Server of Newegg determines which cipher is used for encryption and decryption at the transmitter and receiver of the Host Server and Client Computer during the SSL/TLS handshake. A communication link covered by one or more claims of the '730 patent was established between the Host Server and the Client Computer when the Host Server determined that the RC4 encryption algorithm would be used during the SSL/TLS handshake. Data transmitted over the communication link (both from the Client Computer to the Host Server, and from the Host Server to the Client Computer) comprises a sequence of

blocks, and was transmitted as packets in a sequence over the communication link. The Client Computer and the Host Server automatically encrypted and decrypted the data transmitted over the communication link pursuant to the method steps claimed by the ‘730 patent. The Client Computer and the Host Server automatically provided a seed value to the transmitter and receiver that were used to encrypt and decrypt the data transmitted over the communication link. A first sequence of pseudo-random key values was automatically generated at the transmitter (whichever of the Host Server or Client Computer was sending the encrypted information) to encrypt the data based on said seed values, each new key value in said being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Newegg has encrypted data and transmitted data from the Host Server to the Client Computer over said link. In addition, by using its Host Server to determine that the RC4 encryption algorithm would be used, Newegg has induced users of the Client Computer to encrypt and transmit data over said link to the Host Server. Newegg has generated, and, by using its Host Server to determine that the RC4 encryption algorithm would be used, has caused the Client Computer to automatically generate a second sequence of pseudo-random key values 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. Newegg has decrypted data sent from the Client Computer over said link in order to use the data, and, by using its Host Server to determine that the RC4 encryption algorithm would be used, has caused the

Client Computer to automatically decrypt data transmitted from the Host Server over said link in order to provide a useable display to the user of the Client Computer. Since at least May 6, 2011, when TQP's Complaint was filed, Newegg has had knowledge of the '730 patent and, by continuing the actions described above, has had the specific intent to induce infringement of the '730 patent pursuant to 35 U.S.C. § 271(b).

8. Paragraph 23 of TQP's Complaint is adopted here pursuant to Fed. R. Civ. P. 10(b) and 10(c). Additionally, and in the alternative, upon information and belief, Defendant QVC has induced infringement of the '730 patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, performing certain steps of the methods claimed by the '730 patent, and advising, encouraging, or otherwise inducing others to perform the remaining steps claimed by the '730 Patent to the injury of TQP. For example, QVC has configured the equipment that hosts its secure websites ("Host Server") (including, without limitation to, quality-s.qvc.com), or caused the Host Server to be configured, to require use of the SSL and/or TLS encryption protocols. An SSL/TLS handshake takes place when, for example, a QVC customer, potential customer, or client connects to a secure QVC website with a computer or mobile device ("Client Computer"). The Host Server of QVC determines which cipher is used for encryption and decryption at the transmitter and receiver of the Host Server and the Client Computer during the SSL/TLS handshake. A communication link covered by one or more claims of the '730 patent was established between the Host Server and the Client Computer when the Host Server determined that the RC4 encryption algorithm would be used during the SSL/TLS handshake. Data transmitted over the communication link (both from the Client Computer to the Host Server, and from the Host Server to the Client

Computer) comprises a sequence of blocks, and was transmitted as packets in a sequence over the communication link. The Client Computer and the Host Server automatically encrypted and decrypted the data transmitted over the communication link pursuant to the method steps claimed by the '730 patent. The Client Computer and the Host Server automatically provided a seed value to the transmitter and receiver that were used to encrypt and decrypt the data transmitted over the communication link. A first sequence of pseudo-random key values was automatically generated at the transmitter (whichever of the Host Server or Client Computer was sending the encrypted information) to encrypt the data based on said seed values, 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. QVC has encrypted data and transmitted data from the Host Server to the Client Computer over said link. In addition, by using its Host Server to determine that the RC4 encryption algorithm would be used, QVC has induced users of the Client Computer to encrypt and transmit data over said link to the Host Server. QVC has generated, and, by using its Host Server to determine that the RC4 encryption algorithm would be used, has caused the Client Computer to automatically generate a second sequence of pseudo-random key values 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. QVC has decrypted data sent from the Client Computer over said link in order to use the data, and, by using its Host Server to determine that the RC4 encryption algorithm would be used, has caused the Client Computer to automatically decrypt data transmitted from the Host Server over said link in order to provide a useable display to the user of the Client Computer. Since at least May 6, 2011, when TQP's Complaint was filed, QVC has had knowledge of the '730 patent and, by continuing the actions described above, has had the specific intent to induce infringement of the '730 patent pursuant to 35 U.S.C. § 271(b).

9. Paragraphs 26 through 28 of TQP's Complaint are adopted here pursuant to Fed. R. Civ. P. 10(b) and 10(c).

PRAYER FOR RELIEF

The Prayer for Relief of TQP's Complaint is adopted here pursuant to Fed. R. Civ. P. 10(b) and 10(c), and TQP respectfully requests that this Court enter a judgment in favor of Plaintiff that Defendants have infringed directly, jointly, by directing and controlling the accused encryption process, and/or indirectly by way of inducing the performance of the claimed method steps.

DEMAND FOR JURY TRIAL

The Demand for Jury Trial of TQP's Complaint is adopted here pursuant to Fed. R. Civ. P. 10(b) and 10(c).

Dated: July 22, 2013

Respectfully submitted,

TQP DEVELOPMENT, LLC

By: /s/ *Adams S. Hoffman*
Marc A. Fenster, CA Bar No. 181067
E-mail: mfenster@raklaw.com
Adam S. Hoffman, CA Bar No. 218740
E-mail: ahoffman@raklaw.com
Alexander C. Giza, CA Bar No. 212327
E-mail: agiza@raklaw.com

Paul A. Kroeger, CA Bar No. 229074
Email: pkroeger@raklaw.com
RUSS AUGUST & KABAT
12424 Wilshire Boulevard, 12th Floor
Los Angeles, CA 90025
Telephone: 310/826-7474
Facsimile: 310/826-6991

Andrew W. Spangler, TX Bar No. 24041960
E-mail: spangler@sfipfirm.com
James A. Fussell, III, AR Bar No. 2003193
E-mail: fussell@sfipfirm.com
SPANGLER & FUSSELL 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

CERTIFICATE OF SERVICE

I hereby certify that the counsel of record who are deemed to have consented to electronic service are being served on July 22, 2013, 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.

/s/*Adam S. Hoffman*
Adam S. Hoffman