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

TQP DEVELOPMENT, LLC,	§	
	§	
v.	§	Case No. 2:11-CV-248-JRG-RSP
	§	CONSOLIDATED
1-800-FLOWERS.COM, INC., et al.	§	

CLAIM CONSTRUCTION
MEMORANDUM AND ORDER

On March 12, 2013, the Court held a hearing to determine the proper construction of the disputed claim terms in United States Patent No. 5,412,730. After considering the arguments made by the parties at the hearing and in the parties' claim construction briefing (Dkt. Nos. 172, 178, and 192), the Court issues this Claim Construction Memorandum and Order.

TABLE OF CONTENTS

BACKGROUND

Plaintiff asserts United States Patent No. 5,412,730 ("the '730 Patent"), titled "Encrypted Data Transmission System Employing Means for Randomly Altering the Encryption Keys." The '730 Patent issued on May 2, 1995, and claims priority to a patent application filed on October 6, 1989. Defendants submit that the '730 Patent has expired. Dkt. No. 180 at 1.

The Court has construed the '730 Patent four times: *TQP Development, LLC v. Merrill Lynch & Co., Inc., et al.*, No. 2:08-CV-471, Dkt. No. 383 (E.D. Tex. Mar. 28, 2011) ("*Merrill Lynch I*"); *id.*, Dkt. No. 512 (May 19, 2012) ("*Merrill Lynch II*"); *TQP Development, LLC v. Barclays PLC, et al.*, No. 2:09-CV-88, Dkt. 165 (E.D. Tex. Mar. 28, 2011) ("*Barclays*"); and *TQP Development, LLC v. Ticketmaster Entertainment, Inc.*, No. 2:09-CV-279, Dkt. No. 232 (E.D. Tex. Sept. 23, 2011) ("*Ticketmaster*").

In general, the '730 Patent relates to secure communication through the use of pseudo-random encryption keys. A sequence of pseudo-random keys is generated based on a seed value and an algorithm, and keys are selected depending upon the message data that is being sent over the transmission medium. The transmitter and receiver are thereby able to generate the same sequence of keys without the security risk of transmitting keys from the transmitter to the receiver or vice versa. The term "pseudo-random" means that the sequence has no apparent regularities unless the seed value and algorithm are known or determined. *Merrill Lynch I* at 23; Dkt. No. 172 at 2-3. The abstract of the '730 Patent states:

> A modem suitable for transmitting encrypted data over voice-grade telephone line. The modem is implemented by the combination of integrated circuit components including a microprocessor, a serial communications controller which communicates with connected data terminal equipment, and a modulator/demodulator for translating between voice band tone signals and digital data. Pseudo random number generators are employed at both the transmitting and receiving stations to supply identical sequences of encryption keys to a transmitting encoder and a receiving decoder. An initial random number

> seed value is made available to both stations. The random number generators are advanced at times determined by predetermined characteristics of the data being transmitted so that, after transmission has taken place, the common encryption key can be known only to the transmitting and receiving stations.

The '730 Patent, in its original form, contained one independent claim and one dependent claim. An Ex Parte Reexamination Certificate issued on September 20, 2011, confirming the original claims and adding eight more dependent claims.

Claim 1 of the '730 Patent recites:

> 1. A method for transmitting data comprising a sequence of blocks in encrypted form over a communication link from a transmitter to a receiver comprising, in combination, the steps of:
>
> providing a seed value to both said transmitter and receiver,
>
> generating a first sequence of pseudo-random key values 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,
>
> encrypting the data sent over said link at said transmitter in accordance with said first sequence,
>
> generating a second sequence of pseudo-random key values based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon said predetermined characteristic of said data transmitted over said link such that said first and second sequences are identical to one another[,] a new one of said key values in said first and said second sequences being produced each time a predetermined number of said blocks are transmitted over said link, and
>
> decrypting the data sent over said link at said receiver in accordance with said second sequence.

APPLICABLE LAW

"It is a 'bedrock principle' of patent law that 'the claims of a patent define the invention to which the patentee is entitled the right to exclude.'" *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc) (quoting *Innova/Pure Water Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004)). To determine the meaning of the claims, courts start by considering the intrinsic evidence. *See id.* at 1313; *C.R. Bard, Inc. v. U.S. Surgical Corp.*, 388 F.3d 858, 861 (Fed. Cir. 2004); *Bell Atl. Network Servs., Inc. v. Covad Commc'ns Group,*

Inc., 262 F.3d 1258, 1267 (Fed. Cir. 2001). The intrinsic evidence includes the claims themselves, the specification, and the prosecution history. *See Phillips*, 415 F.3d at 1314; *C.R. Bard*, 388 F.3d at 861. Courts give claim terms their ordinary and accustomed meaning as understood by one of ordinary skill in the art at the time of the invention in the context of the entire patent. *Phillips*, 415 F.3d at 1312-13; *Alloc, Inc. v. Int'l Trade Comm'n*, 342 F.3d 1361, 1368 (Fed. Cir. 2003).

The claims themselves provide substantial guidance in determining the meaning of particular claim terms. *Phillips*, 415 F.3d at 1314. First, a term's context in the asserted claim can be very instructive. *Id.* Other asserted or unasserted claims can aid in determining the claim's meaning because claim terms are typically used consistently throughout the patent. *Id.* Differences among the claim terms can also assist in understanding a term's meaning. *Id.* For example, when a dependent claim adds a limitation to an independent claim, it is presumed that the independent claim does not include the limitation. *Id.* at 1314-15.

"[C]laims 'must be read in view of the specification, of which they are a part.'" *Id.* (quoting *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc)). "[T]he specification 'is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.'" *Id.* (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)); *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1325 (Fed. Cir. 2002). This is true because a patentee may define his own terms, give a claim term a different meaning than the term would otherwise possess, or disclaim or disavow the claim scope. *Phillips*, 415 F.3d at 1316. In these situations, the inventor's lexicography governs. *Id.* The specification may also resolve the meaning of ambiguous claim terms "where the ordinary and accustomed meaning of the words used in the claims lack

sufficient clarity to permit the scope of the claim to be ascertained from the words alone." *Teleflex*, 299 F.3d at 1325. But, "'[a]lthough the specification may aid the court in interpreting the meaning of disputed claim language, particular embodiments and examples appearing in the specification will not generally be read into the claims." *Comark Commc'ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1187 (Fed. Cir. 1998) (quoting *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1571 (Fed. Cir. 1988)); *accord Phillips*, 415 F.3d at 1323. The prosecution history is another tool to supply the proper context for claim construction because a patent applicant may also define a term in prosecuting the patent. *Home Diagnostics, Inc., v. Lifescan, Inc.*, 381 F.3d 1352, 1356 (Fed. Cir. 2004) ("As in the case of the specification, a patent applicant may define a term in prosecuting a patent.").

Although extrinsic evidence can be useful, it is "less significant than the intrinsic record in determining the legally operative meaning of claim language." *Phillips*, 415 F.3d at 1317 (quoting *C.R. Bard*, 388 F.3d at 862). Technical dictionaries and treatises may help a court understand the underlying technology and the manner in which one skilled in the art might use claim terms, but technical dictionaries and treatises may provide definitions that are too broad or may not be indicative of how the term is used in the patent. *Id.* at 1318. Similarly, expert testimony may aid a court in understanding the underlying technology and determining the particular meaning of a term in the pertinent field, but an expert's conclusory, unsupported assertions as to a term's definition are entirely unhelpful to a court. *Id.* Generally, extrinsic evidence is "less reliable than the patent and its prosecution history in determining how to read claim terms." *Id.*

In general, prior claim construction proceedings involving the same patents-in-suit are "entitled to reasoned deference under the broad principles of *stare decisis* and the goals

articulated by the Supreme Court in *Markman*, even though *stare decisis* may not be applicable *per se*." *Maurice Mitchell Innovations, LP v. Intel Corp.*, No. 2:04-CV-450, 2006 WL 1751779, at *4 (E.D. Tex. June 21, 2006). The Court nonetheless conducts an independent evaluation during claim construction proceedings. *See, e.g., Texas Instruments, Inc. v. Linear Techs. Corp.*, 182 F. Supp. 2d 580, 589-90 (E.D. Tex. 2002); *Burns, Morris & Stewart Ltd. P'ship v. Masonite Int'l Corp.*, 401 F. Supp. 2d 692, 697 (E.D. Tex. 2005); *Negotiated Data Solutions, Inc. v. Apple, Inc.*, No. 2:11-CV-390, 2012 WL 6494240 (E.D. Tex. Dec. 13, 2012).

CONSTRUCTION OF AGREED TERMS

Term	Construction
"based on said seed value"	"based exclusively on said seed value"
"associating different ones of seed values with each of a plurality of remote locations with which secured communication is required"	"when secured communication is required with two or more remote locations, associating a different seed value with each of the remote locations"
"associating with each of a plurality of remote locations with which secured communication is required different seed values"	"when secured communication is required with two or more remote locations, associating, at the transmitter, a different seed value with each of the remote locations"
"encrypting the data"	"converting clear text data into cipher text"
"decrypting the data"	"converting cipher text into clear text"
"pseudo-random key values"	"a sequence of numbers that are generated by supplying a seed value to an algorithm, the sequence of numbers have no apparent regularities unless the seed value and algorithm are known or determined"
"said provided seed value is one of a number of seed values for a plurality of remote locations with which secured communication is required"	"when secured communication is required with two or more remote locations, providing more than one seed value for a number of the remote locations for which secured communication is required"

Dkt. No. 172 at 2-3.

CONSTRUCTION OF DISPUTED TERMS

As a preliminary matter, Plaintiff's opening brief proposed, without argument, that the Court adopt several of its prior constructions. *See* Dkt. No. 172 at 3-4. Defendants, in their response brief, stated that as to the terms "data being transmitted over said link" and "predetermined number of said blocks," Plaintiff "did not include these terms as disputed terms requiring construction in the Local P.R. 4-3 Joint Claim Construction and Prehearing Statement." Dkt. No. 180 at 3 n.2. Defendants requested that the Court "defer ruling on these two terms until the parties have an opportunity to confer on them and raise focused disputes, if any, to the Court." *Id.* at 4 n.2. In its reply brief, Plaintiff did not address these two terms apart from the construction of larger terms (*see* Dkt. No. 192), and the parties did not address these two terms at the March 12, 2013 hearing. The two terms at issue therefore need not be construed.

A. "seed value"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
No construction necessary	"initial value"

Dkt. No. 172 at 13.

(1) The Parties' Positions

Plaintiff argues that "Defendants' construction is confusing and unnecessary." Dkt. No. 172 at 13. Plaintiff also notes that in the preferred embodiment, "the seed value is not the 'initial value' for this sequence, instead [it] is what determines what will be the initial value in the sequence." *Id.* Plaintiff further urges that Defendants' proposed construction "would potentially confuse the jury between the seed value supplied prior to decryption and the 'first sequence' of key values that are generated . . . ." *Id.*

Defendants respond that the specification consistently uses the term "seed value" to refer to an "initial" value that is provided in advance. Dkt. No. 180 at 6. Defendants also rely upon "the generally-understood meaning of 'seed'" as meaning a "source or beginning; a germ." *Id.* at 7 (citing Ex. C, *The American Heritage Dictionary of the English Language* 1633 (3d ed. 1992)). Defendants also cite a technical dictionary that defines "seed" as "[a]n initial number used by an algorithm such as a random number generator." *Id.* at 7-8 (citing Ex. F, *McGraw-Hill Dictionary of Scientific and Technical Terms* 1782 (5th ed. 1994)). Defendants emphasize that "the seed value is not 'any' value, but rather is confirmed in the claims and throughout the specification to be the 'initial' value used to generate the keys." *Id.* at 9. Finally, Defendants note that "although the phrases 'providing a seed value to both said transmitter and receiver' and 'based on said seed value' were construed in previous cases, the Court did not address the meaning of 'seed value' within that phrase." *Id.*

Plaintiff replies that "replacing the word 'seed' with 'initial,'" as Defendants have proposed, "does not appear to provide any further clarification." Dkt. No. 192 at 9. Plaintiff reiterates that "Defendants' construction would potentially confuse the jury between the seed value supplied prior to decryption and the 'first sequence' of key values that are generated to decrypt . . . ." *Id.* at 10.

At the March 12, 2013 hearing, Defendants urged that in order to fully address the parties' dispute, the Court's construction should explain that the seed value is not generated as part of the key generation process. In response, Plaintiff cited *PPG Industries v Guardian Industries Corp.*, 156 F.3d 1351 (Fed. Cir. 1998), for the proposition that "after the court has defined the claim with whatever specificity and precision is warranted by the language of the

claim and the evidence bearing on the proper construction, the task of determining whether the construed claim reads on the accused product is for the finder of fact." *Id.* at 1355.

(2) Analysis

Although Plaintiff argues that this term should not be construed, the briefing demonstrates that the parties have a "fundamental dispute regarding the scope of a claim term," and the Court has a duty to resolve the dispute. *O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 1362-63 (Fed. Cir. 2008).

Claim 1 recites, in relevant part (emphasis added):

> 1. A method for transmitting data comprising a sequence of blocks in encrypted form over a communication link from a transmitter to a receiver comprising, in combination, the steps of:
>
> providing a *seed value* to both said transmitter and receiver,
>
> generating a first sequence of pseudo-random key values based on said *seed value* at said transmitter, . . .
>
> generating a second sequence of pseudo-random key values based on said *seed value* at said receiver, ...

The Abstract of the '730 Patent states that "[a]n initial random number seed value is made available to both [the transmitting and receiving] stations." The specification discloses "seed values" multiple times, including in the context of an initial key:

> In accordance with a principle feature of the present invention, pseudo-random number generators are employed at both the transmitting and receiving stations to supply a like sequence of encryption keys to both the encryptor and decryptor, without these keys being transmitted in any form over the transmission facility. In accordance with the invention, to permit the two stations to communicate, each [is] supplied in advance with a *random number seed value* which exclusively determines the numerical content of the sequence of numeric values generated by each of the two pseudo-random generators.

'730 Patent at 1:37-48 (emphasis added).

> Once the host station has supplied the *initial seed value keys* to the units forming the two terminal locations for a given link and transmission over that link begins, the host . . . no longer "knows" the encryption key values since they are dependent upon the nature of the transmissions over the link. Consequently, link

> security cannot be compromised even by an "insider" who is in possession of the initial key values supplied by the host.

Id. at 2:17-25 (emphasis added).

> *The random number generators 23 and 38 at the transmitting station obtain their seed values from a key memory 50*. Key memory 50 stores the *random number keys* indexed by destination (along with telephone dial-up numbers for automatic dialing). Similarly, at the receiving station, *the seed values for the remote terminals from which the receiving station is authorized to receive information are stored in a key memory 60 connected to supply seed values to the generators 27 and 40.* The key memories eliminate[] the need for authorized users to remember and enter *keys* before each transmission or reception.

Id. at 9:51-62 (emphasis added).

> [K]nowledge of the *initial seed values* supplied by the host are of no further value and cannot be used to monitor ongoing communications over the authorized link.

Id. at 11:5-8 (emphasis added).

These disclosures suggest that the "seed value" may be an initial key in the preferred embodiment, but such a limitation should not be imported into the term "seed value" as used in the claims. *Comark Commc'ns*, 156 F.3d at 1187; *accord Phillips*, 415 F.3d at 1323. Defendants' proposal of "initial value," which might be read to require that the "seed value" is itself a key, is therefore hereby expressly rejected.

Nonetheless, the claim language and the above-quoted portions of the specification are consistent with Defendants' argument that the "seed value" is provided in advance of key generation and, therefore, is not created as part of the claimed key generation process. Any other interpretation would read the word "seed" out of the claim. Thus, the plain meaning of "seed value" is appropriate, but the Court provides additional explanation, as follows:

The Court hereby construes **"seed value"** to have its **plain meaning**. The Court further hereby finds, as part of its construction: **"The seed value is provided to the transmitter prior to generating the first sequence of pseudo-random key values, and the seed value is provided to the receiver prior to generating the second sequence of pseudo-random key values."**

B. "providing a seed value to both said transmitter and receiver"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"providing the same seed value to both the transmitter and receiver"	"supplying the same seed value to both said transmitter and receiver in advance of the first contact between the transmitter and receiver from a source other than the transmitter and receiver"

Dkt. No. 172 at 7.

(1) The Parties' Positions

Plaintiff argues that here as in *Merrill Lynch* and *Ticketmaster*, the Court should reject Defendants' attempt "to add a limitation that the seed value be provided 'from outside the transmitter and receiver' and to provide a temporal limitation as to when the seed value must be provided." Dkt. No. 172 at 8. First, Plaintiff submits that "[t]he claims do not place any limitation on where the seed value originates." *Id.* Second, Plaintiff urges that "[a]lthough the transmitter would be required to have the seed value to generate the encryption keys prior to transmission, there is no explicit requirement in the patent or file history that suggests that the receiver must also be provided the seed value prior to transmission." *Id.* at 9.

Defendants respond that because the claims require "providing" the seed value, it must come from a source external to both the transmitter and the receiver. Dkt. No. 180 at 10. Defendants also argue that because the transmitter and receiver must use the same seed value and

because "it is impossible for the same seed values to organically come into existence in both the transmitter and receiver," "they must originate from the same source, outside those devices." *Id.* at 11-12.

In reply, Plaintiff reiterates that *Merrill Lynch I* and *Ticketmaster* rejected proposals "to add (1) a limitation that the seed value be provided 'from outside the transmitter and receiver' and (2) a temporal limitation as to when the seed value must be provided." Dkt. No. 192 at 5. Plaintiff also notes that "at the time the seed value is provided to the transmitter and receiver it is located in the key memory stored within those items." *Id.* at 5. Finally, Plaintiff urges that "[t]he invention of the ['730] Patent would function as described as long as the seed value was provided to the receiver any time *prior to decrypting* the encrypted data sent over the link." *Id.* at 5-6.

At the March 12, 2013 hearing, the parties discussed Figures 1 and 4. Whereas Figure 1 depicts a seed value entering the transmitter and the receiver, Figure 4 does not. Plaintiff argued that Figure 4 thereby illustrates a seed value being internally generated. Defendants responded that Figure 4 does not depict any internal generation and, moreover, the specification discloses that the key memories shown in Figure 4 obtain the seed value from an external source.

(2) Analysis

In *Merrill Lynch I*, the Court noted disclosure with reference to Figure 4 that seed values could be obtained from "key memory 50" within "transmitting station 11" and "key memory 60" within "receiving station 12." *Merrill Lynch I* at 18-19. In *Ticketmaster*, the Court found that "[a]lthough[] the transmitter would be required to have the seed value to generate the encryption keys prior to transmission, there is no explicit requirement in the patent or file history that suggests that the receiver must also be provided the seed value prior to transmission."

Ticketmaster at 9; *see id.* at 12. *Ticketmaster* found, instead, that "[t]he invention of the '730 patent would likewise function if the seed value was provided to the receiver any time prior to decrypting the encrypted data sent over the link." *Id.* at 9; *see id.* at 12.

The specification discloses that the transmitter and receiver must be provided with the seed value in order to perform their respective functions:

> In accordance with the invention, to permit the two stations to communicate, each [is] supplied in advance with a random number seed value which exclusively determines the numerical content of the sequence of numeric values generated by each of the two pseudo-random generators. In order that the two generators switch from one output key value to the next in synchronism, means are employed at both the transmitting and receiving stations to monitor the flow of transmitted data and to advance the random number generator each time the transmitted data satisfies a predetermined condition.

'730 Patent at 1:43-53.

> Once the host station has supplied the initial seed value keys to the units forming the two terminal locations for a given link and transmission over that link begins, the host . . . no longer "knows" the encryption key values since they are dependent upon the nature of the transmissions over the link. Consequently, link security cannot be compromised even by an "insider" who is in possession of the initial key values supplied by the host.

Id. at 2:17-25.

> Of course, in order for the receiving station to successfully decipher the incoming cipher text, the receiving station 12 must be provided (in some fashion) with both the correct seed value and the correct interval number. These values are supplied to the receiving station in advance of the transmission by any secure means.

Id. at 4:13-20.

> Data signals from the DTE [(data terminal equipment)] which are to be transmitted are encrypted as described above and shown in FIG. 1, the random number seed values and the interval number values being pre-supplied to the microprocessor 101 and stored in memory subsystem 103.

Id. at 5:15-19.

> The random number generators 23 and 38 at the transmitting station obtain their seed values from a key memory 50. Key memory 50 stores the random number keys indexed by destination (along with telephone dial-up numbers for automatic

> dialing). Similarly, at the receiving station, the seed values for the remote terminals from which the receiving station is authorized to receive information are stored in a key memory 60 connected to supply seed values to the generators 27 and 40. The key memories eliminate[] the need for authorized users to remember and enter keys before each transmission or reception.

Id. at 9:51-60.

> A switch operated by a physical key is also advantageously included in each station unit and has "security enabled" and "security disabled" positions. The key memory can only be loaded with values identifying one or more remote units with whom communications are authorized when the switch is in the "security disabled" position (typically when the unit is being set up by an authorized operator who has the physical key needed to disable the security switch). At that time, the table can be loaded either from a remote (host) station or by a local command which takes the form of an extension to the standard modem AT command set. That load command take the form:
>
> AT JSN KDESKEY PHONENUM
>
> where AT is the AT command prefix, JSN is the letter "J" immediately followed by the serial number of the remote station with which communications is authorized, KDESKEY is the letter "K" immediately followed by an 8 character DES encryption key, and PHONENUM is the standard routing code (e.g. dial-up phone number string). In the preferred embodiment, up to 1000 serial numbers and keys, and up to 100 optional dial-up phone number strings (each with up to 39 digits) may [be] stored in the key memory lookup table.

Id. at 10:21-46.

> In accordance with an important feature of this arrangement, the host system may initially authorize communication between two connected units by supplying the appropriate serial numbers and initial key values (unique to an authorized link), but as soon as transmission begins between the two units over the authorized link, the encryption keys are changed in ways that are unknowable to the host. As a consequence, knowledge of the initial seed values supplied by the host are of no further value and cannot be used to monitor ongoing communications over the authorized link.

Id. at 10:66-11:8.

Figures 1 and 4 of the ‘730 Patent are reproduced here:

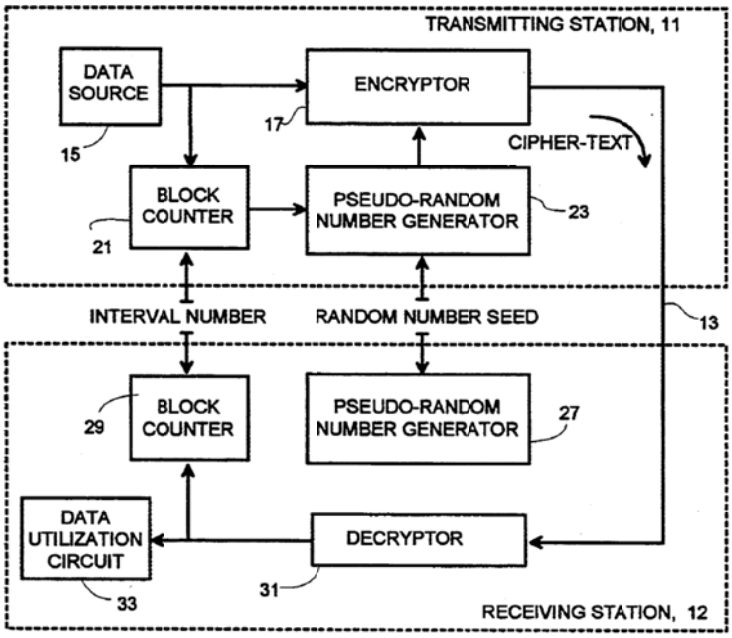

Fig. 1

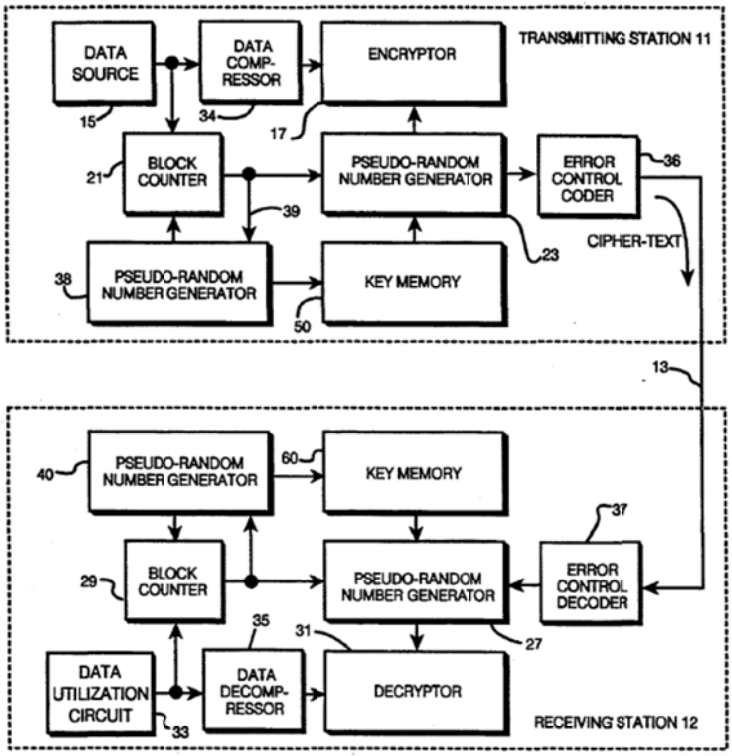

Fig. 4

On balance, Defendants have failed to justify their proposed limitation that the seed value must be provided to both the transmitter and the receiver before any contact between them. Instead, the above-quoted portions of the specification contemplate that the seed value need only be provided before any encrypted communication can be accomplished between the transmitter and the receiver. To that end, the seed value must be provided to the transmitter before a communication can be encrypted and must be provided to the receiver before the encrypted communication can be decrypted. Defendants' proposal to limit the claims to a preferred embodiment is hereby expressly rejected. *Comark Commc'ns*, 156 F.3d at 1187; *accord Phillips*, 415 F.3d at 1323.

Similarly, Defendants have failed to justify their proposed limitation that the seed value must be provided by a source other than either the transmitter or the receiver. The claim language does not recite a separate source. Further, Defendants have not shown that the claimed use of a pseudo-random sequence of encryption keys, which is based in part on the transmitted data, necessarily precludes the seed value from being provided by the transmitter or the receiver. As noted by the specification, once the seed value is provided and communication has commenced, the communication is secure, even if an intruder knows the seed value. *See* '730 Patent at 10:66-11:8. In short, the origin of the seed value is not a limitation of the claim. Defendants' proposal to limit the claims to a preferred embodiment is hereby expressly rejected. *Comark Commc'ns*, 156 F.3d at 1187; *see Phillips*, 415 F.3d at 1323.

The Court therefore hereby construes **"providing a seed value to both said transmitter and receiver"** to mean **"providing the same seed value to both the transmitter and receiver."**

C. "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"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"a new key value in the first and second sequence is produced each time a predetermined number of blocks are transmitted over the link"	"switching to the next new key value in the first and second sequences of key values each time a predetermined number of blocks have been sent from the transmitter over the communication link"

Dkt. No. 172 at 5.

(1) The Parties' Positions

Plaintiff proposes the construction reached in *Barclay*s. *Barclays* at 18. Plaintiff argues that because key values cannot be "switched" if they have not already been generated, Defendants' proposal improperly requires that key values must be generated in advance. Dkt. No. 172 at 5. Plaintiff submits that "Defendants' proposal also improperly excludes the possibility, inconsistent with the specification, that multiple key values are generated at the same time." *Id.* at 6. Finally, Plaintiff argues that Defendants' proposal that "blocks have been sent from the transmitter over the communication link" is "redundant and unnecessary." *Id.*

Defendants respond that although *Barclays* construed the disputed term, "two important requirements were not addressed in that proceeding: what it means to (1) 'produce' a new key value in the sequence (2) each time blocks 'are transmitted.'" Dkt. No. 180 at 14. Defendants argue that "coordinated 'switching' of key values is critical to the invention, as it allows the transmitter and receiver to stay in sync." *Id.* Defendants further argue that the claims and the specification consistently explain that "the key value is not changed until after the blocks being counted have been transmitted." *Id.* at 17. Finally, Defendants argue that Plaintiff's proposed construction repeats the constituent terms "produced" and "transmitted" and thus fails to resolve the parties' dispute. *Id.* at 17 n.12.

Plaintiff replies by reiterating its opening arguments and by urging that Defendants' proposal adds an improper temporal limitation because "[t]here is nothing to 'switch' to if the key values have not yet been produced." Dkt. No. 192 at 2.

(2) Analysis

Claim 1 recites (emphasis added):

> 1. A method for transmitting data comprising a sequence of blocks in encrypted form over a communication link from a transmitter to a receiver comprising, in combination, the steps of:
>
> providing a seed value to both said transmitter and receiver,
>
> generating a first sequence of pseudo-random key values 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,
>
> encrypting the data sent over said link at said transmitter in accordance with said first sequence,
>
> generating a second sequence of pseudo-random key values based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon said predetermined characteristic of said data transmitted over said link such that said first and second sequences are identical to one another[,] *a new one of said key values in said first and said second sequences being produced each time a predetermined number of said blocks are transmitted over said link*, and
>
> decrypting the data sent over said link at said receiver in accordance with said second sequence.

In *Barclays*, the court agreed with Plaintiff's argument that "what is important is that each key be *used* at precisely the right time relative to the data. It does not matter whether that key is generated at that time, or pre-generated and stored." *Barclays* at 16; *see id.* at 17. *Barclays* construed the disputed term to mean "a new key value in the first and second sequence is produced each time a predetermined number of blocks are transmitted over the link." *Id.* at 18.

The abstract of the '730 Patent states (emphasis added):

> The *random number generators are advanced* at times determined by predetermined characteristics of the data being transmitted so that, *after transmission has taken place*, the common encryption key can be known only to the transmitting and receiving stations.

The specification discloses counting blocks to determine when to advance to a new key value:

> In accordance with a principle feature of the present invention, pseudo-random number generators are employed at both the transmitting and receiving stations to supply a like sequence of encryption keys to both the encryptor and decryptor, without these keys being transmitted in any form over the transmission facility. In accordance with the invention, to permit the two stations to communicate, each [is] supplied in advance with a random number seed value which exclusively determines the numerical content of the sequence of numeric values generated by each of the two pseudo-random generators. *In order that the two generators switch from one output key value to the next in synchronism, means are employed at both the transmitting and receiving stations to monitor the flow of transmitted data and to advance the random number generator each time the transmitted data satisfies a predetermined condition.*
>
> The monitoring function can advantageously be performed simply by *counting the units of data being transmitted and by advancing each pseudo-random key generator each time the count reaches an agreed-upon interval number*. In this way, no additional synchronization information needs to be added to the data stream. For even greater security, the interval number (which must be reached before the key is switched) may itself be a changing value generated by a random number generator, so that the duration during which a given key is active changes from key to key at times which are predictable only by the authorized recipient.

'730 Patent at 1:37-65 (emphasis added).

> The advance signal produced by block counter 21 is supplied to the advance input of a pseudo-random number generator 23 which *supplies a sequence of encryption key values to the key input of the encryptor 17*. The content of the key sequence is predetermined by the combination of (1) the internal makeup of the generator 23 and by (2) a supplied random number seed value which initializes the generator 23. *The generator 23 responds to each advance signal from block counter 21 by changing its output to the next successive encryption key value.* Thus, for example, the combination of counter 21 and generator 23 operate to *change the encryption key each time* [*the*] *total number of bytes transmitted is an exact multiple of the predetermined interval number*.
>
> * * *
>
> The block counter 21 need not supply advance signals on boundaries between encryption units, nor does the generator 23 need to provide new key value precisely on encryption unit boundaries. Instead, the encryptor 17 may *buffer the new key*[] *temporarily*, using it for the first time on the next successive encryption unit of data.
>
> * * *

> *Block counter 29* performs the identical function as that performed by the counter 21 at the transmitting station 11 and hence *supplies advance signals to the generator 27 at precisely the same times (relative to the data stream) that counter 21 advances generator 23*. Each time the current count reaches the interval number, the pseudo-random number generator 27 is advanced. Since the internal makeup of random number generator 27 is identical to that of generator 23, and since it is supplied with the same seed value, and since block counter 29 is supplied with the same interval number value as that supplied to the block counter 21, exactly the same sequence of keys will be supplied to the random number generators 23 and 27, and *the keys will change at precisely the same time* (relative to the data stream) to accurately decipher the transmitted data.

Id. at 3:26-40, 3:50-56 & 3:64-4:12 (emphasis added).

Thus, the '730 Patent refers to "a sequence of encryption key values" and also to "advanc[ing] the random number generator," when a certain number of data units have been transmitted, so as to use a new encryption key. *See id.* at Abstract, 1:37-65 & 3:26-40. On balance, nothing in the '730 Patent precludes generating a sequence of encryption key values in advance and then using the key values at appropriate times. As found in *Barclays*, Claim 1 does not specify whether the key is generated at the time of use or is generated ahead of time and then selected at the time of use. *Barclays* at 17 ("The claim further only requires that each new key be 'produced' at a specific time relative to the data. It does not matter whether that key is generated at that time, or pre-generated and stored."). To the extent Defendants are proposing that the new key value cannot be created until after the predetermined number of blocks have been transmitted, Defendants' proposal is hereby expressly rejected.

Finally, as to the determination of whether "a predetermined number of said blocks" have been "transmitted over said link," the claim explicitly refers to transmission, not to encryption or to some other step of preparing for transmission.

The Court therefore hereby construes **"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"** to mean **"a new key value in the first and second sequence is used each time a predetermined number of blocks have been sent from the transmitter over the communication link."**

D. "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" and "each new key value in said sequence being produced at a time dependent upon said predetermined characteristic of said data transmitted over said link"

"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"	
Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"a new key value in the first sequence is produced each time a condition based on a predetermined characteristic of the transmitted data is met at the transmitter"	"each new key value in the first sequence is produced each time a predetermined number of blocks are transmitted over said link"
"each new key value in said sequence being produced at a time dependent upon said predetermined characteristic of said data transmitted over said link"	
Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"a new key value in the second sequence is produced each time a condition based on a predetermined characteristic of the transmitted data is met at the receiver"	"each new key value in the second sequence is produced each time a predetermined number of blocks are transmitted over said link"

Dkt. No. 172 at 6; Dkt. No. 180 at 17.

(1) The Parties' Positions

Plaintiff proposes the constructions reached by the Court in *Merrill Lynch I* and *Ticketmaster*. *Merrill Lynch I* at 26-27; *Ticketmaster* at 17-18. Plaintiff argues that "Defendants' proposed construction would effectively exclude th[e] preferred embodiment which provides the new key value based upon a varying interval number and not a 'predetermined number of blocks.'" Dkt. No. 172 at 7.

Defendants respond that producing a new key value based on an "interval number" of blocks transmitted over the communications link is "a critical aspect of the claimed invention" because "it enables the transmitter and the receiver to switch from one key value to the next in sync with each other, without transmitting any additional information in the data stream across the communications link." Dkt. No. 180 at 19. As to Figure 4 of the '730 Patent, Defendants respond that "[a]lthough the embodiment depicted in Figure 4 allows for the interval number to actively vary over the course of a series of transmissions (['730 Patent] at 8:7-15, 9:29-50), the interval number is still under all circumstances a predetermined number of blocks that have been transmitted over the link." Dkt. No. 180 at 21. Defendants further cite Plaintiff's response to a motion for summary judgment in one of the present consolidated cases, in which Plaintiff stated: (1) the "predetermined characteristics relate to the 'correct interval number' described in some embodiments of the specification"; (2) "'interval numbers' are represented in the claims by 'predetermined characteristic[s] of the data being transmitted' and 'predetermined number of said blocks'"; and (3) "the claimed method includes 'interval numbers' as part of the claim language requiring 'predetermined characteristic of the data'/'predetermined number of said blocks . . . .'" *Id.* at 21-22 (citing Case No. 2:12-CV-55, Dkt. No. 53 at 9-10 & 12; *id.*, Dkt. No. 59 at 9-10).

Plaintiff replies by reiterating that "Defendants' proposed construction would effectively exclude th[e] preferred embodiment [shown in Figure 4], which provides the new key value based upon a varying interval number and not a 'predetermined number of blocks.'" Dkt. No. 192 at 4. Plaintiff also highlights disclosure in the specification that "the predetermined condition can be satisfied after counting 'the number of bytes (characters), words, or blocks of data transmitted.'" *Id.* (quoting '730 Patent at 3:20-21). As to the summary judgment briefing

cited by Defendants, Plaintiff replies that it "noted that the 'interval number' was the 'predetermined characteristic' in 'some embodiments,'" not necessarily in all embodiments. *Id.* at 4 n.1 (citing Dkt. No. 180 at 21).

(2) Analysis

Claim 1 recites (emphasis added):

> 1. A method for transmitting data comprising a sequence of blocks in encrypted form over a communication link from a transmitter to a receiver comprising, in combination, the steps of:
>
> providing a seed value to both said transmitter and receiver,
>
> generating a first sequence of pseudo-random key values 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,*
>
> encrypting the data sent over said link at said transmitter in accordance with said first sequence,
>
> generating a second sequence of pseudo-random key values based on said seed value at said receiver, *each new key value in said sequence being produced at a time dependent upon said predetermined characteristic of said data transmitted over said link such that said first and second sequences are identical to one another*[,] a new one of said key values in said first and said second sequences being produced each time a predetermined number of said blocks are transmitted over said link, and
>
> decrypting the data sent over said link at said receiver in accordance with said second sequence.

In *Merrill Lynch I*, the Court clarified that the first disputed phrase relates to the first sequence and the transmitter and the second disputed phrase relates to the second sequence and the receiver. *Merrill Lynch I* at 26.

The background of the invention states:

> The monitoring function can advantageously be performed simply by counting the units of data being transmitted and by *advancing each pseudo-random key generator each time the count reaches an agreed-upon interval number*.

'730 Patent at 1:54-58 (emphasis added). The specification discloses that the "interval number" may be constant or may change every time the encryption key value is advanced:

> A block counter 21 monitors the stream of data from the source 15 and generates an "advance signal" each time the data meets a predetermined condition. Advantageously, the block counter 21 may simply count the number of bytes (characters), words or blocks of data being transmitted, compare the current count with a predetermined 37 ["]interval number" and produce an advance signal each time the current count reaches the interval number (at which time the current count is reset to 0).
>
> *The advance signal produced by block counter 21 is supplied to the advance input of a pseudo-random number generator 23 which supplies a sequence of encryption key values to the key input of the encryptor 17.* The content of the key sequence is predetermined by the combination of (1) the internal makeup of the generator 23 and by (2) a supplied random number seed value which initializes the generator 23. *The generator 23 responds to each advance signal from block counter 21 by changing its output to the next successive encryption key value.* Thus, for example, the combination of counter 21 and generator 23 operate to change the encryption key each time [the] total number of bytes transmitted is an exact multiple of the predetermined interval number.

Id. at 3:16-40 (emphasis added).

> To further enhance the security of the transmission, *the duration of the interval during which each given key is active may be changed in a pseudo-random fashion*. For this purpose, a pseudo-random number generator 38 is used at the transmitting station 11 to supply the interval numbers to the block counter 21. The generator 38 is advanced to a new number each time an advance signal is received from the output of block counter 21 over line 39 (so that a new interval number is supplied to the block counter 21 each time it advances the encryption key generator 23). Block counter 21 may simply load the interval number from generator 38 into an accumulator which is then decremented toward zero when it emits the advance signal to generator 23, at which time it is loaded with a new and different interval number from generator 38. At the receiving station 12, a pseudo-random generator 40 (which performs the same pseudo-random number generating process as the generator 38 at the transmitting station 11) supplies a sequence of interval numbers to counter 29. Generator 40 is advanced by the advance signals from counter 29 which also advance the encryption key generator 27.

Id. at 9:29-50 (emphasis added).

As to the prosecution history, Defendants have cited an amendment in which the applicant cancelled the original claims and added new claims containing the disputed terms. Dkt. No. 180, Ex. T, 12/4/1992 Amendment at 2. On balance, the prosecution history contains no "definitive" statements that limit the scope of the disputed terms. *Omega Eng. v. Raytek*

Corp., 334 F.3d 1314, 1324 (Fed. Cir. 2003) ("As a basic principle of claim interpretation, prosecution disclaimer promotes the public notice function of the intrinsic evidence and protects the public's reliance on *definitive* statements made during prosecution.") (emphasis added). In particular, Defendants have not shown how this amendment warrants limiting "predetermined characteristic of said data" to mean a "predetermined number of blocks."

On balance, Defendants' proposal to limit the disputed terms to the preferred embodiments that employ an "interval number" is hereby rejected. *Comark Commc'ns*, 156 F.3d at 1187; *see Phillips*, 415 F.3d at 1323. Moreover, even if an interval number limitation were appropriate, reference to a "predetermined number of blocks" might be read to exclude embodiments that use a varying interval between key value changes rather than a static, predetermined interval. *Id.* at 9:29-50; *see id.* at Fig. 4. Defendants' proposed constructions are therefore hereby expressly rejected.

The Court accordingly hereby construes the disputed terms as set forth in the following chart:

Term	Construction
"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"	**"a new key value in the first sequence is produced each time a condition based on a predetermined characteristic of the transmitted data is met at the transmitter"**
"each new key value in said sequence being produced at a time dependent upon said predetermined characteristic of said data transmitted over said link"	**"a new key value in the second sequence is produced each time a condition based on a predetermined characteristic of the transmitted data is met at the receiver"**

E. "sequence of blocks in encrypted form"

Plaintiff's Proposed Construction	Defendants' Proposed Construction
No construction necessary[1]	"a sequence of blocks, encrypted together using the same key value for transmission, which signals to change the encryption key"

Dkt. No. 172 at 13; Dkt. No. 180 at 23.

(1) The Parties' Positions

Plaintiff argues that based on the Court's prior construction of the term "block" to mean "a group of bits, such as a character, word, or other unit of data," a "sequence of blocks" is simply a sequence of groups of bits. Dkt. No. 172 at 14. Plaintiff also argues that contrary to Defendants' proposal, nothing in the claim language or the specification requires that every transmission of a "sequence of blocks" must change the encryption key. *Id.* In particular, Plaintiff submits that "the preferred embodiment could change its key after counting the blocks from multiple transmission[s], and not just one." *Id.*

Defendants respond that the Court has not previously considered the present dispute, which is whether "the claimed 'sequence of blocks in encrypted form' must be encrypted together with the same key," as Defendants propose. Dkt. No. 180 at 23 (emphasis omitted). Defendants argue that "[b]ecause the encryption key does not change until a predetermined number or sequence of blocks is transmitted, the blocks in each sequence of blocks are encrypted together with the same key." *Id.* at 23-24.

Plaintiff replies that "the preferred embodiment can change its key after counting the blocks from multiple transmissions, and not just one." Dkt. No. 192 at 10. Plaintiff also argues

[1] Plaintiff submits that the disputed term is simply "sequence of blocks." Dkt. No. 172 at 13.

that Defendants' proposal that only a predetermined number of blocks can change the encryption key is contrary to the disclosed embodiments in which the number of blocks can vary. *Id.*

At the March 12, 2013 hearing, Plaintiff emphasized that as to the term "said blocks," which appears in the disputed term discussed in subsection C., above, the antecedent basis for "said blocks" is "blocks," not "sequence."

(2) Analysis

As a threshold matter, the parties do not appear to dispute the meaning of the constituent term "sequence." That term can therefore be used in the Court's construction without any elaboration.

In *Merrill Lynch I* and *Barclays*, the Court construed the constituent term "block" to mean "a group of bits, such as a character, word, or other unit of data." *Merrill Lynch I* at 16; *Barclays* at 8.

Claim 1 recites (emphasis added):

> 1. A method for transmitting data comprising a *sequence of blocks in encrypted form* over a communication link from a transmitter to a receiver comprising, in combination, the steps of:
>
> providing a seed value to both said transmitter and receiver,
>
> generating a first sequence of pseudo-random key values 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,
>
> encrypting the data sent over said link at said transmitter in accordance with said first sequence,
>
> generating a second sequence of pseudo-random key values based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon said predetermined characteristic of said data transmitted over said link such that said first and second sequences are identical to one another[,] *a new one of said key values in said first and said second sequences being produced each time a predetermined number of said blocks are transmitted over said link*, and
>
> decrypting the data sent over said link at said receiver in accordance with said second sequence.

The specification discloses using a particular key to encrypt segments of data, advancing the key to a new value, and using the new key to encrypt more data:

> In order that the two generators switch from one output key value to the next in synchronism, means are employed at both the transmitting and receiving stations to monitor the flow of transmitted data and to advance the random number generator each time the transmitted data satisfies a predetermined condition.
>
> * * *
>
> Thus, for example, the combination of counter 21 and generator 23 operate to change the encryption key each time [the] total number of bytes transmitted is an exact multiple of the predetermined interval number.
>
> The encryptor 17 translates fixed length segments of the data from source 15 ("clear text") into fixed-length "cipher text" output segments, each segment translation taking place in a manner uniquely determined by the encryption key currently supplied by the pseudo-random number generator 23.

'730 Patent at 1:50-58 & 3:36-46.

Defendants' proposed construction appears to require multiple blocks. On one hand, use of a plural term does not always mandate a plurality. For example:

> In the phrase "[plurality of . . .] projections with recesses therebetween," the use of "recesses" can be understood to mean a single recess where there are only two projections and more than one recess where there are three or more projections. Indeed, in the present context, if the patentees had wanted to require . . . more than one recess, it would have been natural to limit the claimed invention to an insert means with a "plurality of recesses."

Dayco Prods, Inc. v. Total Containment, Inc., 258 F.3d at 1328; *see Versa Corp. v. Ag-Bag Int'l Ltd.*, 392 F.3d 1325, 1330 (Fed. Cir. 2004) (as to the term "means . . . for creating air channels," noting that "in context, the plural can describe a universe ranging from one to some higher number, rather than requiring more than one item").

On the other hand, the plural form of a noun generally refers to two or more, as found in *Markem-Imaje Corp. v. Zipher Ltd.*, 657 F.3d 1293, 1297 (Fed. Cir. 2011), and *Leggett & Platt, Inc. v. Hickory Springs Manufacturing Co.*, 285 F.3d 1353, 1357 (Fed. Cir. 2002). The Court

addressed these cases and other relevant cases in *Calypso Wireless, Inc., et al. v. T-Mobile USA, Inc.*, No. 2:08-CV-441, Dkt. No. 281 at 27-32 (E.D. Tex. Dec. 3, 2012) (discussing *Flash Seats, LLC v. Paciolon, Inc.*, No. 07-575-JJF, 2010 WL 184080 (D. Del. Jan. 19, 2010), *aff'd*, 469 Fed. App'x 916 (Fed. Cir. 2012), *Every Penny Counts, Inc. v. Bank of Am. Corp.*, No. 2:07-CV-42-FTM-29SPC, 2008 WL 4491113 (M.D. Fla. Sept. 29, 2008), and *MOAEC, Inc. v. Pandora Media, Inc.*, No. 07-CV-654-BBC, 2008 WL 4500704 (W.D. Wis. Sept. 30, 2008)).

Thus, the use of the plural form of "blocks" in Claim 1 of the '730 Patent weighs in favor of finding that two or more blocks are required. *Leggett & Platt*, 285 F.3d at 1357 ("At the outset, the claim recites 'support wires' in the plural, thus requiring more than one welded 'support wire.'"). Nothing in the '730 Patent is contrary to such a natural reading.

As to the prosecution history, Defendants have submitted that in response to a rejection, the applicant narrowed "data" to "data comprising a sequence of blocks," and added "a new one of said key values in said first and said second sequences being produced each time a predetermined number of said blocks are transmitted over said link[.]" Dkt. No. 180 at 24 (citing Ex. P, 7/8/1993 Office Action at 2; Ex. Y, 12/13/1993 Amendment After Final at 1-2). Nonetheless, Defendants have not identified any definitive statement by the patentee that all of the blocks in a "sequence of blocks" must be encrypted using the same key value. *Omega Eng.*, 334 F.3d at 1324 ("As a basic principle of claim interpretation, prosecution disclaimer promotes the public notice function of the intrinsic evidence and protects the public's reliance on *definitive* statements made during prosecution.") (emphasis added).

Finally, Defendants' proposal (that the recited "sequence" is encrypted using the same key) would seem to require that every time a key new value is produced, all of the steps recited in Claim 1 must be performed again. Such an interpretation might arise from the preamble,

which recites: "A method for transmitting data comprising a sequence of blocks in encrypted form . . . ." If the entire sequence is encrypted using the same key, then production of a new key must relate to transmission of a new sequence. Defendants have not argued that "a sequence" must refer to at least two sequences, so to the extent the claim encompasses transmission of a single sequence, the production of a new key might be read to require performing all of the recited steps again, including providing a seed value. Requiring a new seed value upon every key change would be inconsistent with the specification and even the claim language itself, which contemplates synchronized advancement through a sequence of key values that have been generated from a common seed value. Defendants' proposal, which would thus render the claim confusing and potentially inconsistent with itself and the specification, is accordingly disfavored.

On balance, none of the evidence warrants requiring that all of the blocks in the recited "sequence of blocks" must be encrypted using the same key. Defendants' proposal in that regard is hereby expressly rejected.

The Court therefore hereby construes **"sequence of blocks in encrypted form"** to mean **"sequence of two or more blocks that have been encrypted."**

F. "predetermined"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
No construction necessary	"determined before any transmission over said communication link"

Dkt. No. 172 at 10; Dkt. No. 180 at 25.

(1) The Parties' Positions

Plaintiff argues that "[t]he term 'predetermined' is a commonly used term and does not need any construction" and "simply means to determine beforehand." Dkt. No. 172 at 11 (citing Ex. E, *Merriam-Webster Dictionary* (on-line version)). Plaintiff cites the finding in *Ticketmaster*

that "neither the claim language nor specification requires that the claimed 'predetermined' characteristic or claimed 'predetermined' number of blocks be 'determined before any transmission,' instead it only requires that these be determined in advance of 'any communications,' not transmissions." *Ticketmaster* at 23.

Defendants respond that "[a]ccording to the claims and specification, the 'determining' must occur before the encrypted transmissions commence." Dkt. No. 180 at 25. As to Plaintiff's reliance on *Ticketmaster*, Defendants submit they have no opposition to substituting "communication" for "transmission" in their proposed construction. *Id.* at 26.

Plaintiff replies by again emphasizing *Ticketmaster*. Dkt. No. 192 at 8.

(2) Analysis

Although Plaintiff argues that this term should not be construed, the briefing demonstrates that the parties have a "fundamental dispute regarding the scope of a claim term," and the Court has a duty to resolve the dispute. *O2 Micro*, 521 F.3d at 1362-63.

Claim 1 recites (emphasis added):

> 1. A method for transmitting data comprising a sequence of blocks in encrypted form over a communication link from a transmitter to a receiver comprising, in combination, the steps of:
>
> providing a seed value to both said transmitter and receiver,
>
> generating a first sequence of pseudo-random key values 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,
>
> encrypting the data sent over said link at said transmitter in accordance with said first sequence,
>
> generating a second sequence of pseudo-random key values based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon said *predetermined* characteristic of said data transmitted over said link such that said first and second sequences are identical to one another[,] a new one of said key values in said first and said second sequences being produced each time a *predetermined* number of said blocks are transmitted over said link, and

decrypting the data sent over said link at said receiver in accordance with said second sequence.

The specification discloses that for encryption and decryption to occur, certain information must be provided to the transmitter and the receiver "in advance":

> In accordance with the invention, to permit the two stations to communicate, each [is] *supplied in advance* with a random number seed value which exclusively determines the numerical content of the sequence of numeric values generated by each of the two pseudo-random generators. In order that the two generators switch from one output key value to the next in synchronism, means are employed at both the transmitting and receiving stations to monitor the flow of transmitted data and to advance the random number generator each time the transmitted data satisfies a predetermined condition.
>
> The monitoring function can advantageously be performed simply by counting the units of data being transmitted and by advancing each pseudo-random key generator each time the count reaches an agreed-upon interval number. In this way, no additional synchronization information needs to be added to the data stream.

'730 Patent at 1:43-59 (emphasis added).

> *Once the host station has supplied the initial seed value keys to the units forming the two terminal locations for a given link and transmission over that link begins,* the host . . . no longer "knows" the encryption key values since they are dependent upon the nature of the transmissions over the link. Consequently, link security cannot be compromised even by an "insider" who is in possession of the initial key values supplied by the host.

Id. at 2:17-25 (emphasis added).

> Of course, in order for the receiving station to successfully decipher the incoming cipher text, the receiving station 12 must be provided (in some fashion) with both the correct seed value and the correct interval number. *These values are supplied to the receiving station in advance of the transmission by any secure means.*

Id. at 4:13-20.

As found in *Ticketmaster*, these disclosures, as well as the plain language of the claim, are consistent with construing "predetermined" to refer to a determination that occurs before any communication involving data comprising a sequence of blocks that have been encrypted using the recited pseudo-random key values. Otherwise, the recited sequences of pseudo-random keys

could not be generated and, in turn, the data could not be encrypted. Finally, at the March 12, 2013 hearing, Plaintiff's counsel stated that "predetermined" refers to the same point in time regardless of whether the term is being used with respect to the transmitter or with respect to the receiver.

The Court therefore hereby construes **"predetermined"** to mean **"determined before any communication of a sequence of encrypted blocks."**

G. "data"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
No construction necessary	"serial data"

Dkt. No. 172 at 12.

(1) The Parties' Positions

Plaintiff argues that "data" is a "broad term" and "[n]othing in the claim language requires the data be transmitted, encrypted or decoded in a series." Dkt. No. 172 at 12.

Defendants respond that the claims recite transmission of a "sequence" of data blocks, which refers to serial data rather than parallel data. Dkt. No. 180 at 26. Defendants note that the applicant added this "sequence" language to the claim during prosecution. *See id.*, Ex. Y, 12/13/1993 Amendment After Final Rejection at 1-2.

Plaintiff replies that "Defendants improperly seek to import a limitation from the preferred embodiment to the claims by noting that the preferred embodiment makes use of a 'serial communication control,' a 'serial port,' 'serial interface,' and 'serial protocol.'" Dkt. No. 192 at 9.

(2) Analysis

In *Barclays*, the parties, including Plaintiff, agreed that the preamble phrase "A method for transmitting data comprising a sequence of blocks in encrypted form over a communication link from a transmitter to a receiver comprising, in combination, the steps of" is a limitation of the claim. *Barclays* at 9.

The specification discloses "data" multiple times, including in the context of serial communication:

> The monitoring function can advantageously be performed simply by counting the *units of data* being transmitted and by advancing each pseudo-random key generator each time the count reaches an agreed-upon interval number.

'730 Patent at 1:54-58 (emphasis added).

> At the transmitting station 11, a source of data 15 supplies a *serial data stream* to the data input of an encryptor 17.

Id. at 3:11-13 (emphasis added).

> The encryptor 17 translates fixed length segments of the *data* from source 15 ("clear text") into fixed-length "cipher text" output segments, each segment translation taking place in a manner uniquely determined by the encryption key currently supplied by the pseudo-random number generator 23. The encryptor 17 (and the decryptor 19, to be discussed) may advantageously employ the accepted NBIS Data Encryption Standard (DES), which codes and decodes *data* in 64-bit (8 byte) units in accordance with a 56-bit key. The block counter 21 need not supply advance signals on boundaries between encryption units, nor does the generator 23 need to provide new key value precisely on encryption unit boundaries. Instead, the encryptor 17 may buffer the new key[] temporarily, using it for the first time on the next successive encryption unit of *data*.

Id. at 3:40-56 (emphasis added).

> The asynchronous *serial interface* with the DTE typically operates under the combined control of the microprocessor 101 and the SCC 111 in accordance with a standard interface protocol (e.g., the V.42 standard protocol). The DTE (data terminal equipment) may be any terminal or computer adapted to communicate via this standard port using the selected serial protocol.

Id. at 4:65-5:4 (emphasis added).

> As mentioned above, the data terminal equipment (DTE) communicates with the modem hardware over the *serial port* 121 (e.g., a RS-232c or a RS-422 standard port).

Id. at 5:62-65 (emphasis added).

> [E]rror control processing (such as adding cyclic redundancy check (CRC) block checking codes) is best done after encryption in accordance with the invention, because successful synchronization of the advance signals from the block counters 21 and 29 requires substantially error-free *data* transmission (which the error-checking protocols insure).

Id. at 8:22-28 (emphasis added).

On balance, the term "data" is used generically and has not been imbued with any special meaning. The disclosure of "serial data" pertains to a preferred embodiment and is not required by any claim language or any definitive statements in the specification or the prosecution history. *Comark Commc'ns*, 156 F.3d at 1187; *accord Phillips*, 415 F.3d at 1323; *see Omega Eng.*, 334 F.3d at 1324. Defendants' proposal to limit "data" to serial data is therefore rejected.

The Court accordingly hereby construes **"data"** to have its **plain meaning**, and the Court hereby expressly rejects Defendants' proposal to limit "data" to "serial data."

H. "block"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"a group of bits, such as a character, word, or other unit of data"	"fixed length segment of the data"

Dkt. No. 172 at 9.

(1) The Parties' Positions

Plaintiff proposes the construction reached by the Court in *Merrill Lynch I*. *Merrill Lynch I* at 16. Plaintiff argues that the claim language specifies no "fixed length" and that the specification discloses a block counter that may count units, words, or blocks of data of any size. Dkt. No. 172 at 10.

Defendants respond that the specification describes encryption as being performed upon "fixed length segments of the data." Dkt. No. 180 at 28 (citing '730 Patent at 3:41-46). Defendants also argue that "[t]he patent's description of block counting as being compression-sensitive further supports Defendants' proposed construction." Dkt. No. 180 at 28. Defendants further argue that Plaintiff's position is inconsistent with the prosecution history, in which the patentee "limit[ed] the scope of 'data' to 'data comprising a sequence of blocks,' to overcome the examiner's final rejection." *Id.* (citing Ex. Y, 12/13/1993 Amendment After Final Rejection at 1-2).

Plaintiff replies that the specification discloses that "a block counter may count 'groups of bits' of varying sizes or units of data, words, or blocks of data of any other size." Dkt. No. 192 at 7 (citing '730 Patent at 1:54-58 & 3:19-25). Plaintiff also submits that *Merrill Lynch I* rejected the same prosecution history argument that Defendants are advancing here. *Id.* (citing *Merrill Lynch I* at 17).

(2) Analysis

As the Court stated in *Merrill Lynch I*, "the specification does not provide an explicit definition of the term 'blocks.'" *Merrill Lynch I* at 10; *see id.* at 12. As to the prosecution history, *Merrill Lynch I* noted: "The Court agrees that the applicant did limit the term 'data.' However, what is unclear from the prosecution history is exactly how the term 'data' was narrowed by the amendment." *Id.* at 13. *Merrill Lynch I* found that "contrary to Defendants' contention, it is unclear from the intrinsic record if the only defining feature of a block with which to narrow the term 'data' is length." *Id.* at 14 (internal citation and quotation marks omitted). Having considered the intrinsic evidence as well as extrinsic definitions submitted by the parties, *Merrill Lynch I* concluded that rather than specifying any particular length, "the term

'block' narrowed the term 'data' by requiring the data to be a group of bits, such as a character, word, or other unit of data." *Id.* at 16.

The specification discloses various different groupings of data, and those groupings may indeed be fixed-length:

> The monitoring function can advantageously be performed simply by counting the *units of data* being transmitted and by advancing each pseudo-random key generator each time the count reaches an agreed-upon interval number.

'730 Patent at 1:54-58 (emphasis added).

> *The data from source 15 may take substantially any form, such as a file of text characters, each encoded as a 8-bit byte, or a file of numerical binary information expressed in 16-bit or 32-bit words.* A block counter 21 monitors the stream of data from the source 15 and generates an "advance signal" each time the data meets a predetermined condition. Advantageously, the block counter 21 may simply count the number of bytes (characters), words or blocks of data being transmitted, compare the current count with a predetermined 37 ["]interval number" and produce an advance signal each time the current count reaches the interval number (at which time the current count is reset to 0).

Id. at 3:13-25 (emphasis added).

> *The encryptor 17 translates fixed length segments of the data from source 15 ("clear text") into fixed-length "cipher text" output segments,* each segment translation taking place in a manner uniquely determined by the encryption key currently supplied by the pseudo-random number generator 23.

Id. at 3:41-46 (emphasis added).

> Note also that, as depicted in FIG. 4, the data is monitored by the block counter 21 prior to compression, rather than afterwards. Correspondingly, at the receiving station 12, the block counter 29 monitors the data flow after it is decompressed. In this way, both counters monitor the same data stream. Both could be reconnected to monitor the compressed data stream if desired, however.

Id. at 9:12-19.

On balance, the claimed invention depends upon the transmitter and receiver counting blocks in the same manner, but nothing in the '730 Patent requires that the blocks must be fixed-length. The above-quoted discussion of "fixed length segments" (*id.* at 3:41-46) thus relates to a

preferred embodiment, and Defendants' proposal, which would import that limitation into the claims, is hereby expressly rejected. *Comark Commc'ns*, 156 F.3d at 1187; *accord Phillips*, 415 F.3d at 1323.

The Court therefore hereby construes **"block"** to mean **"a group of bits, such as a character, word, or other unit of data."**

I. "communication link from a transmitter to a receiver"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
No construction necessary	"a connection for communication between a transmitter and a receiver"

Dkt. No. 172 at 11.

(1) The Parties' Positions

Plaintiff argues that no construction is necessary because "the language is plain and can be easily understood and applied by the jury." Dkt. No. 172 at 11. Plaintiff also argues that "Defendants' attempt to rewrite the claim language from a 'communication link from a transmitter to a receiver' to 'a connection for communication between a transmitter and a receiver' finds no support in the specification." *Id.* at 12.

Defendants respond that their proposal "clarifies that a link from a transmitter and a receiver is a connection between those two points." Dkt. No. 180 at 29. Defendants urge that "[t]he communication channel or link must be the connection between the transmitting and receiving station—rather than a part of the transmitting and receiving stations—otherwise the claim language would contradict the specification." *Id.* at 30. Finally, Defendants submit that "[c]ontrary to [Plaintiff's] assertions, Defendants' proposed construction does not require a 'direct' connection, but simply clarifies that the claimed link is between a transmitter and a receiver." *Id.*

Plaintiff replies that the "communication link 13" shown in Figures 1 and 4 of the '730 Patent is simply an arrow, and Plaintiff argues that "[n]othing in the specification or claims requires a 'connection' between the transmitter and receiver, simply that communications from one reach the other." Dkt. No. 192 at 8.

(2) Analysis

The specification discloses:

> FIG. 1 illustrates the manner in which the data being transmitted is subjected to a sequence of signal processing steps as contemplated by the present invention. These processing steps are executed at *a transmitting station 11 and at a receiving station 12 connected to opposite ends of a communications channel 13*.

Id. at 3:5-10 (emphasis added).

On balance, Defendants' proposed construction is unnecessary and would do little, if anything, to clarify the disputed term. Instead, the claim language is sufficiently clear such that the disputed term need not be construed. *U.S. Surgical Corp. v. Ethicon, Inc.*, 103 F.3d 1554, 1568 (Fed. Cir. 1997) ("Claim construction is a matter of resolution of disputed meanings and technical scope, to clarify and when necessary to explain what the patentee covered by the claims, for use in the determination of infringement. It is not an obligatory exercise in redundancy."); *see O2 Micro*, 521 F.3d at 1362 ("[D]istrict courts are not (and should not be) required to construe every limitation present in a patent's asserted claims."). To whatever extent Defendants are proposing that the "communication link" must be a wired connection or must be a direct connection (without any intermediate devices), Defendants' proposal is hereby expressly rejected.

The Court therefore hereby construes **"communication link from a transmitter to a receiver"** to have its **plain meaning**.

CONCLUSION

The Court adopts the above constructions. The parties are ordered that they may not refer, directly or indirectly, to each other's claim construction positions in the presence of the jury. Likewise, the parties are ordered to refrain from mentioning any portion of this opinion, other than the actual definitions adopted by the Court, in the presence of the jury. Any reference to claim construction proceedings is limited to informing the jury of the definitions adopted by the Court.