UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/573,627	10/05/2009	Hayo Parduhn	0057-024001/2009P00165US	6539

56056 7590 06/18/2018
BRAKE HUGHES BELLERMANN LLP
C/O CPA Global
900 Second Avenue South
Suite 600
MINNEAPOLIS, MN 55402

EXAMINER
ZELASKIEWICZ, CHRYSTINA E

ART UNIT	PAPER NUMBER
3621	

NOTIFICATION DATE	DELIVERY MODE
06/18/2018	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@brakehughes.com
docketing@brakehughes.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte HAYO PARDUHN, MARK MICHAUD,
MARKUS BECKER, INGO BRAEUNINGER,
STEFAN LEONHARDT, JEAN BERBERIAN,
BERND LEHNERT, and BERND SIEREN

Appeal 2017-001472
Application 12/573,627
Technology Center 3600

Before JUSTIN BUSCH, CATHERINE SHIANG, and
CARL L. SILVERMAN, *Administrative Patent Judges*.

BUSCH, *Administrative Patent Judge*.

DECISION ON APPEAL

Pursuant to 35 U.S.C. § 134(a), Appellants appeal from the Examiner's decision to reject claims 10–18 and 21–31, which constitute all the claims pending in this application. We have jurisdiction over the pending claims under 35 U.S.C. § 6(b). We affirm.

CLAIMED SUBJECT MATTER

Appellants' invention is directed to "securely transferring sensitive data across a system landscape." Spec. ¶ 1. Appellants' systems or methods combine "all sensitive information found in a transaction data log (TLOG)

. . . into one segment and the segment is encrypted once," allowing the target system to extract all of the sensitive information while only performing a single decryption operation. *Id.* ¶ 16. Claims 10, 21, and 31 are independent claims. Claim 10 is illustrative and reproduced below:

> 10. A computer system comprising:
>
> at least one memory storing instructions; and
>
> at least one processor configured to execute the instructions which, when executed, cause the computer system to perform operations including:
>
> receiving transaction data in a first computerized system, the transaction data including a plurality of sections, each section including a section reference, wherein a first section contains first encrypted payment data and a first section reference and a second section contains second encrypted payment data, and a second section reference,
>
> decrypting the first encrypted payment data and the second encrypted payment data;
>
> generating a file having a first portion including the first decrypted payment data and the first section reference and a second portion including the second decrypted payment data and the second section reference, the second portion being appended to the first portion;
>
> encrypting the file using a first encryption algorithm;
>
> generating an encrypted data segment, the encrypted data segment including the encrypted file, and unencrypted information about the first encryption algorithm; and
>
> sending the encrypted data segment with the transaction data to a second computerized system, the second computerized system accessing the first payment data by decrypting the file using the first encryption algorithm and matching the first section reference in the decrypted data segment to the first section reference in the transaction data.

REJECTIONS

Claims 10–18 and 21–31 stand rejected under 35 U.S.C. § 101 as being directed to ineligible subject matter. Final Act. 2–3.

Claims 10–18 and 21–28 stand rejected under 35 U.S.C. § 103(a) as obvious in view of von Mueller (US 2011/0211689 A1; Sept. 1, 2011) and Ching (US 2005/0273440 A1; Dec. 8, 2005). Final Act. 3–7.

Claim 29 stands rejected under 35 U.S.C. § 103(a) as obvious in view of von Mueller, Ching, Hogg (US 2012/0130783 A1; May 24, 2012), and Ruano (US 2006/0224470 A1; Oct. 5, 2006). Final Act. 7–9.

Claims 30 and 31 stand rejected under 35 U.S.C. § 103(a) as obvious in view of von Mueller, Ching, and Hogg. Final Act. 9–11.

ANALYSIS

We have reviewed the Examiner's rejections in light of Appellants' arguments that the Examiner erred. In reaching this decision, we have considered all evidence presented and all arguments Appellants made. Arguments Appellants could have made, but chose not to make in the Briefs, are deemed waived. *See* 37 C.F.R. § 41.37(c)(1)(iv).

THE § 101 REJECTION

The Examiner concludes claims 10–18 and 21–31 are directed to judicially excepted subject matter. Final Act. 2–3; Ans. 3–9.

Alice/Mayo Framework

The Patent Act defines patent-eligible subject matter broadly: "Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title." 35 U.S.C. § 101. There is no dispute that claims 1–21 are directed to one of these categories.

In *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, 566 U.S. 66, 70 (2012), and *Alice*, 134 S. Ct. at 2354, the Supreme Court explained that 35 U.S.C. § 101 "contains an important implicit exception" for laws of nature, natural phenomena, and abstract ideas. *See Diamond v. Diehr*, 450 U.S. 175, 185 (1981). In *Mayo* and *Alice*, the Court set forth a two-step analytical framework for evaluating patent-eligible subject matter: (1) "determine whether the claims at issue are directed to" a patent-ineligible concept, such as an abstract idea; and, if so, (2) "consider the elements of each claim both individually and 'as an ordered combination' to determine whether the additional elements" add enough to transform the "nature of the claim" into "significantly more" than a patent-ineligible concept. *Alice*, 134 S. Ct. at 2355 (quoting *Mayo*, 566 U.S. at 79); *see Affinity Labs of Tex., LLC v. DIRECTV, LLC*, 838 F.3d 1253, 1257 (Fed. Cir. 2016).

Step one in the *Mayo/Alice* framework involves looking at the "focus" of the claims at issue and their "character as a whole." *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016). Instead of using a definition of an abstract idea, "the decisional mechanism courts now apply is to examine earlier cases in which a similar or parallel descriptive nature can be seen—what prior cases were about, and which way they were decided." *Amdocs (Isr.) Ltd. v. Openet Telecom, Inc.*, 841 F.3d 1288, 1294 (Fed. Cir. 2016) (citing *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1353–54 (Fed. Cir. 2016)); *accord* United States Patent and Trademark Office, *July 2015 Update: Subject Matter Eligibility* (July 30, 2015), https://www.uspto.gov/sites/default/files/

documents/ieg-july-2015-update.pdf (instructing Examiners that "a claimed concept is not identified as an abstract idea unless it is similar to at least one concept that the courts have identified as an abstract idea.").

Step two involves the search for an "inventive concept." *Alice*, 134 S. Ct. at 2355; *Elec. Power*, 830 F.3d at 1353. For an inventive concept, "more is required than 'well-understood, routine, conventional activity already engaged in'" by the relevant community. *Rapid Litig. Mgmt. Ltd. v. CellzDirect, Inc.*, 827 F.3d 1042, 1047 (Fed. Cir. 2016) (quoting *Mayo*, 566 U.S. at 79–80).

Step One of Alice Framework

Turning to step one of the *Alice* framework, the Examiner states "[t]he claims are directed to a series of steps on encrypting/decrypting transaction data, which is a fundamental economic practice and thus an abstract idea." Final Act. 2. The Examiner further concludes the claims are directed to an abstract idea because "sending transaction data and an encrypted data segment to a computer system, wherein the encrypted data segment comprises both information on an algorithm used to encrypt a file and the encrypted file itself . . . is an idea of itself and a fundamental economic practice." Ans. 3; *see id.* at 3–5.

Appellants argue "the claim is focused on generating a data container that improves processing time of transactions in a transaction log at a target computer" and that there is no evidence supporting the Examiner's conclusion that the claims are directed to an abstract idea or that encrypting and decrypting transactions is a fundamental economic practice. App. Br. 9–10. Appellants further assert the Examiner oversimplifies and overgeneralizes the claims without taking into account the improvement provided by the invention. Reply Br. 2–3 (citing *McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1312, 1316 (Fed. Cir. 2016)). Appellants contend the claims recite specific technical features providing a technological improvement to transaction processing and that the claims are deeply rooted in computer networks. Reply Br. 3–4 (citing *McRO*, 837 F.3d at 1316; *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245 (Fed. Cir. 2014)).

Appellants' claims generally relate to decrypting secure data from a plurality of encrypted transactions, repackaging the decrypted data from the plurality of transactions into an aggregate file, and transmitting the aggregate file with the original transactions so that a system receiving the transaction data needs to perform only one decryption to access the secure data. In other words, as the Examiner stated, the claims are directed to a series of steps on encrypting/decrypting transaction data. Appellants' characterization of the claims as being directed to generating a data container that improves the time it may take a target computer to process the plurality of transactions is also accurate. *See Apple, Inc. v. Ameranth, Inc.*, 842 F.3d 1229, 1240 (Fed. Cir. 2016) ("An abstract idea can generally be described at different levels of abstraction.").

The Federal Circuit concluded "a process of organizing information through mathematical correlations" was a patent-ineligible abstract idea. *Digitech Image Techs., LLC v. Elecs. for Imaging, Inc.*, 758 F.3d 1344, 1350 (Fed. Cir. 2014); *see also id.* at 1351 ("Without additional limitations, a process that employs mathematical algorithms to manipulate existing information to generate additional information is not patent eligible.");

Content Extraction, 776 F.3d at 1347 (concluding collecting, recognizing, and storing information is an abstract idea).

Further, merely combining several abstract ideas does not render the combination any less abstract. *RecogniCorp, LLC v. Nintendo Co. Ltd.*, 855 F.3d 1322, 1327 (Fed. Cir. 2017) ("Adding one abstract idea (math) to another abstract idea . . . does not render the claim non-abstract."); *see also FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089, 1093–94 (Fed. Cir. 2016) (determining the pending claims were directed to a combination of abstract ideas).

Although not exactly the same, Appellants' claims are directed to subject matter similar to that claimed in *Digitech* and *Content Extraction*. In particular, Appellants' claims recite receiving data (i.e., transaction data having a plurality of sections), manipulating, or organizing and storing, the data (i.e., decrypting the payment data in the transaction data, organizing all the payment data into a single file, and encrypting the file), and sending data (i.e., sending the transaction data and the encrypted file to a target computer system). *See Digitech*, 758 F.3d at 1344 (concluding "taking existing information . . . and organizing this information into a new form" is an abstract idea); *Content Extraction*, 776 F.3d at 1347; *see also Elec. Power*, 830 F.3d at 1353–54 (concluding "collecting information, analyzing it, and displaying certain results of the collection and analysis," regardless of particular content, is an abstract idea).

Even assuming Appellants' characterization of the claims is correct, we are not persuaded the Examiner erred in concluding the claims are directed to an abstract idea. Appellants' assertion that the claims are directed to "generating a data container that improves processing time of transactions in a transaction log at a target computer" is just another way of stating that the claims relate to "taking existing information . . . and organizing this information into a new form," *Digitech*, 758 F.3d. at 1344) in order to shift the majority of the processing time necessary to decrypt each transaction in a transaction log from the target system to an intermediate computer system.

Contrary to Appellants' arguments, Reply Br. 2–4, the alleged improvement recited in Appellants' claims (i.e., the target system needing to decrypt data only once for the aggregated transaction data rather than decrypting each transaction separately) actually adds an encryption step and a decryption step as compared to the prior art over which Appellants' invention allegedly improves. In particular, the decryption of each transaction still must occur, but Appellants' invention shifts the initial decryption of each transaction to a platform other than the target system, then the platform that decrypted each transaction encrypts a file that aggregates the individual transactions, and the target system decrypts only the aggregate file. Accordingly, although it is true that the *target system* performs only a single decryption step, the process as a whole must still decrypt each transaction *in addition to* encrypting and decrypting each aggregate file generated. Merely shifting where the decryption of each transaction is performed while adding additional encryption and decryption steps does not alter the character of the claims.

For the above reasons, we are unpersuaded the Examiner erred in concluding the claims are directed to an abstract idea.

Step Two of Alice Framework

Next, we turn to step two of *Alice* to determine whether the limitations, when considered both "individually and 'as an ordered combination'" contain an "inventive concept" sufficient to transform the claimed "abstract idea" into a patent-eligible application. *Alice*, 134 S. Ct. at 2355–58. We agree with the Examiner that the additional limitations, separately, or as an ordered combination, do not provide meaningful limitations (i.e., do not add significantly more) sufficient to transform the abstract idea into a patent eligible application. Final Act. 2–3; Ans. 5–7.

The Examiner finds, and we agree, the additional elements are merely generic, routine computer elements that do not add meaningful limitations to the abstract idea and that "single decryption of sensitive information is old and well known in the art (as shown in [the] 103 rejection below)." Final Act. 2–3; *see* Ans. 5–7. More specifically, we agree with the Examiner that reciting a "memory storing instructions," a "processor configured to execute the instructions," and first and second computerized systems that manipulate (i.e., receive, decrypt, generate, encrypt, and send) data represent well-known, conventional, and routine use of memory, processors, and computerized systems. Ans. 7. The Examiner further explains that "[t]he computer components are recited at a high level of generality and perform the basic functions of a computer," and that "[g]enerically recited computer elements do not add a meaningful limitation to the abstract idea." *Id.*; *see Alice*, 134 S. Ct. at 2360 (concluding system claims that "recite a handful of generic computer components configured to implement the" abstract idea recited in the method "add nothing of substance to the underlying abstract idea").

Appellants argue that, "[i]f the abstract idea is merely encrypting business transactions as alleged by the Examiner, then the particular, detailed steps in the remainder of the claim are certainly enough to escape the ineligibility exception under Alice." App. Br. 12. Appellants contend the claims recite "very particular steps [that] must be carried out," rendering the claims more than the "abstract idea of encrypting business transactions" because the claims are more than just "encrypting business transactions" or "'receiving/sending data.'" *Id.* at 13. Appellants further assert the claims are similar to the claims in *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245 (Fed. Cir. 2014), contending Appellants' claims "'do not merely recite the performance of some business practice known from the pre-Internet world along with the requirement to perform it on the Internet,' but rather [are] rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks.'" App. Br. 13–14 (quoting *DDR*, 773 F.3d at 1257).

Appellants, however do not provide persuasive evidence or argument to support their position. *See* App. Br. 14–15. Instead of identifying particular limitations, or an ordered combination of limitations, that allegedly amount to significantly more than the abstract idea itself Appellants merely paraphrase the entirety of claim 1 and assert that "[c]learly, these detailed requirements are enough to render the claim patent-eligible." App. Br. 13. Further, we note the Specification discloses the use of "an existing computer processor" for performing the claimed functions. Spec. ¶ 58, Fig. 1; *see* Spec. ¶¶ 58–62 (describing implementations of the disclosed computer elements as systems using well-known, conventional, and routine generic computing elements). Accordingly, we disagree with Appellants that the claims recite significantly more under step two of *Alice*.

Appellants' claims merely recite using generic computing equipment to receive transaction data including encrypted data and an identifier for each section, decrypt portions of the received data, generate a file with the decrypted information and an identifier for corresponding section, encrypt the generated file, and send the received and generated data, along with information about the encryption algorithm used, to another generic computing system. Appellants' steps involve no more than the routine use of a conventional computer. *See Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335–36 ("[T]he first step . . . asks whether the focus of the claims is on the specific asserted improvement in computer capabilities . . . or, instead, on a process that qualifies as an 'abstract idea' for which computers are invoked merely as a tool."); *see also Alice*, 134 S. Ct. at 2358–59. Here, the focus of the claims is not on an improvement in computers as tools or upon an innovative way to use computers or other devices, but is focused on an independently abstract idea that uses generic, well-understood, conventional, and routine computer and networking elements as tools for their intended purposes.

The fact that the recited process and systems allow the target system to more efficiently decrypt the data it needs by performing the decryption of each segment at an intermediate computer system does not improve a computer or technology, but rather improves the process itself. *See Gottschalk v. Benson*, 409 U.S. 63, 66 (1972) (explaining that the claimed steps could easily "be carried out in existing computers long in use, no new machinery being necessary."). Accordingly, the claimed limitations, considered both individually and together, do not add significantly more to the abstract idea and, therefore, do not render the subject matter patent eligible.

Finally, Appellants argue the claims recite sufficient limitations "to narrow the claim so as not to cover all encryption/decryption of transactions." App. Br. 11–13. "'[W]hile preemption may signal patent ineligible subject matter, the absence of complete preemption does not demonstrate patent eligibility.'" *FairWarning IP*, 839 F.3d at 1098 (quoting *Ariosa Diagnostics, Inc. v. Sequenom, Inc.*, 788 F.3d 1371, 1379 (Fed. Cir. 2015); *see also OIP Techs., Inc. v. Amazon.com, Inc.*, 788 F.3d 1359, 1362–63 (Fed. Cir. 2015) ("[T]hat the claims do not preempt all price optimization or may be limited to price optimization in the e-commerce setting do not make them any less abstract."). Further, "[w]here a patent's claims are deemed only to disclose patent ineligible subject matter under the *Mayo* framework, as they are in this case, preemption concerns are fully addressed and made moot." *Ariosa*, 788 F.3d at 1379.

Summary

For the above reasons, we are unpersuaded of Examiner error. Accordingly, we sustain the Examiner's rejection of independent claims 10, 21, and 31 under 35 U.S.C. § 101. We also sustain the Examiner's rejection of claims 11–18 and 22–30, which depend directly or indirectly therefrom and were not argued separately. *See* App. Br. 7–14; 37 C.F.R. § 41.37(c)(1)(iv)(2016).

THE § 103 REJECTION

The Examiner finds the combination of von Mueller and Ching teaches or suggests the subject matter recited in independent claims 10 and

21 and the combination of von Mueller, Ching, and Hogg teaches or suggests the subject matter recited in independent claim 31. Final Act. 3–5; 8–10.[1] Of particular note, the Examiner finds von Mueller's paragraph 148 teaches or suggests "sending the encrypted data segment with the transaction data to a second computerized system," as recited in independent claims 10, 21, and 31. Final Act. 4. The Examiner reiterates the finding in the Answer and additionally cites paragraphs 270 and 271 of von Mueller, but provides no explanation of the relevance of those paragraphs. Ans. 11.

Paragraph 148 of von Mueller describes different options for handling the previously decrypted bank identification number (BIN) (i.e., either encrypting the BIN or leaving the BIN unencrypted) and further explains that certain embodiments may use separate encryption keys for different parts of the sensitive information so that an encryption key distribution method allows for controlling selective decryption of information at various stages of the process or points in the transaction network. von Mueller ¶ 148. Paragraphs 269 through 271 of von Mueller describe a portion of the "operational flow diagram illustrating a process for processing batch settlements where some or all of the account data has been encrypted, in accordance with one embodiment of the invention." *Id.* ¶ 264, Fig. 20; *see id.* ¶¶ 269–270.

[1] The Examiner cumulatively cites Hogg for the third section. Final Act. 8–10 (citing Hogg ¶¶ 50, 56). Notably, the Examiner finds von Mueller's disclosure of a plurality of transactions in a batch settlement file teaches or suggest the recited "plurality of sections." Final Act. 4 (citing von Mueller ¶ 23). This paragraph does not limit the number of transactions to fewer than three and, to the extent this paragraph teaches or suggests two sections with encrypted payment data, the same disclosure also would at least suggest a third section in the batch settlement file.

Specifically, paragraph 269 describes a portion of the process involving decrypting encrypted data for a given data record in a batch settlement file using the appropriate key that was previously retrieved and returning the decrypted information. *Id.* ¶ 269; *see id.* ¶ 265. If an expiration date field was modified to indelicate the given data record was encrypted, the expiration date can be "returned to its original date and reinserted into the data." *Id.* ¶ 269. The decrypted transaction information is then processed in embodiments where the transaction processor performs the decryption step. *Id.* ¶ 270. In embodiments where an interim server decrypts the transaction information, the interim server forwards the decrypted transaction information to the transaction processor. *Id.* In some embodiments, the interim server may separate transactions from the batch file and send the transactions "individually or in subsets to their respective transaction processors," whereas in other embodiments "the batch file can be reconstructed with the clear text information and sent for processing." *Id.* In embodiments using an interim server to decrypt the transaction information, von Mueller further discloses the interim server may re-encrypt the data before sending it to the transaction processor and provides a non-limiting example of how such encryption regimes can be implemented. *Id.* ¶ 271.

Among other arguments, Appellants contend von Mueller does not teach or suggest "sending the encrypted data segment with the transaction data," as recited in the independent claims. App. Br. 21–22. Appellants note the Examiner maps von Mueller's batch settlement file to the recited "transaction data" and maps re-encrypting that data to the recited "encrypted data segment." App. Br. 22 (citing Final Act. 4). Given the Examiner's findings, Appellants argue von Mueller would need to teach or suggest sending the transaction data twice (i.e., once as the original encrypted batch settlement file and a second time with the re-encrypted batch settlement file). *Id.* Appellants assert neither the additional citations to von Mueller's paragraphs 269 through 271 nor any other aspect of the Answer address this argument. Reply Br. 6.

We agree with Appellants that, based on the current record, the Examiner fails to show that von Mueller teaches or suggests "sending the encrypted data segment with the transaction data to a second" system. As discussed above, the Examiner maps von Mueller's originally encrypted batch settlement file to the recited transaction data and von Mueller's re-encrypted transaction data, which subsequently is included in an encrypted data segment, to the recited encrypted file. *See* Final Act. 4. The Examiner further finds von Mueller's decryption and re-encryption of a subset of the transaction items teaches or suggests the recited generating and encrypting a file steps. Final Act. 4 (citing von Mueller ¶¶ 126–129, 133, 265). Even assuming these findings are correct, the claim recites "sending the encrypted data segment with the transaction data to a second computerized system," and the Examiner has not provided sufficient explanation or evidence demonstrating that von Mueller's re-encrypted transaction data is sent to a second system with the originally encrypted batch settlement file.

As pointed out by Appellants, the Examiner has not shown how von Mueller's disclosure of decrypting and re-encrypting data teaches or suggests sending the recited "encrypted data segment" that includes the recited "file" "with the transaction data," as recited in the claims because von Mueller discloses altering the batch settlement file to create the re-encrypted file (as part of the recited encrypted data segment) and, therefore, does not suggest sending both the re-encrypted data *and* the originally received batch settlement file. Nor does the Examiner sufficiently explain why von Mueller's cited portions would have taught or suggested to a person of ordinary skill in the art to send "the encrypted data segment with the transaction data to a second computerized system," as recited in the independent claims.

Without such explanations or evidence from the Examiner, we are constrained by the record and do not sustain the Examiner's rejection. Accordingly, we are persuaded the Examiner erred in rejecting claims 10 and 21 as obvious in view of von Mueller and Ching. For the same reasons discussed above, we are persuaded the Examiner erred in rejecting claim 31 as obvious in view of von Mueller, Ching, and Hogg. Dependent claims 11–18 and 22–30 ultimately depend from claims 10 and 21, respectively, and incorporate the same limitation recited in claims 10 and 21. The Examiner does not rely on any additional evidence or reasoning to cure the identified deficiency in rejecting the dependent claims. Accordingly, we are persuaded the Examiner erred in rejection dependent claims 11–18 and 22–30 for the same reasons discussed above.

DECISION

We affirm the Examiner's decision to rejection claims 10–18 and 21–31 as directed to ineligible subject matter under 35 U.S.C. § 101.

We reverse the Examiner's decision to reject claims 10–18 and 21–31 under 35 U.S.C. § 103(a).

Because we affirm at least one ground of rejection with respect to each claim on appeal, the Examiner's decision is affirmed. *See* 37 C.F.R. § 41.50(a)(1).

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED