

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

RIGHTQUESTION, LLC,	§	
<i>Plaintiff,</i>	§	
v.	§	CIVIL ACTION NO. 2:24-CV-91-JRG
VERIZON BUSINESS NETWORK	§	(Lead Case)
SERVICES, LLC <i>et al.</i> ,	§	
<i>Defendants.</i>	§	

RIGHTQUESTION, LLC,	§	
<i>Plaintiff,</i>	§	
v.	§	CIVIL ACTION NO. 2:24-CV-94-JRG
AT&T CORP. <i>et al.</i> ,	§	(Member Case)
<i>Defendants.</i>	§	

MEMORANDUM CLAIM CONSTRUCTION OPINION AND ORDER

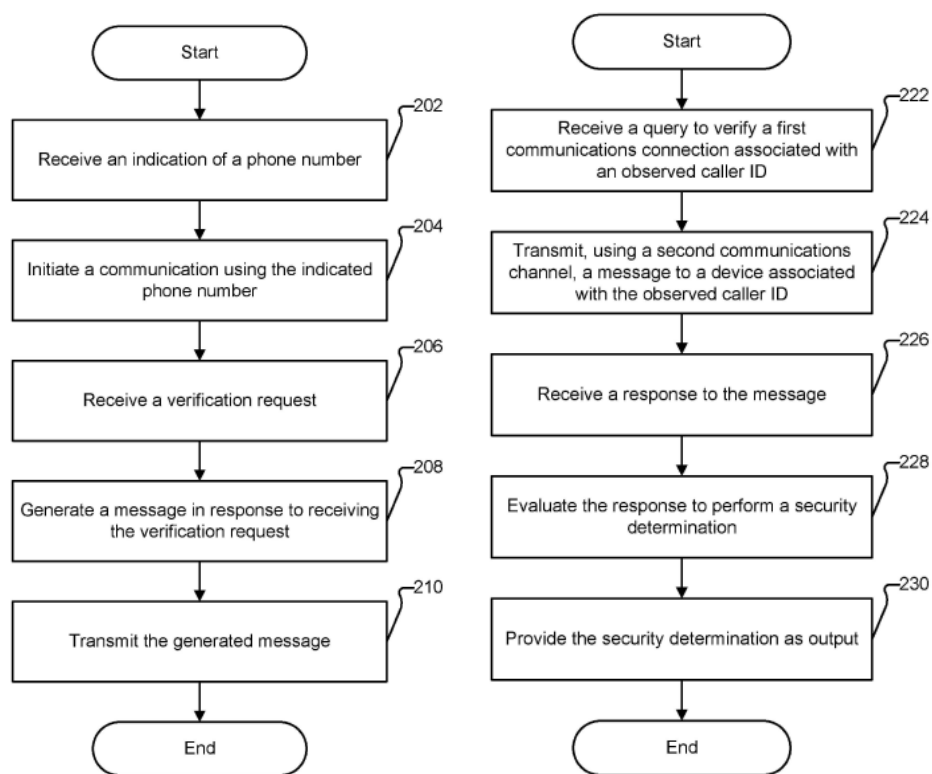
In these consolidated patent cases, RightQuestion, LLC, alleges infringement by Verizon Business Network Services LLC, AT&T Corporation, and several affiliates (together, “Defendants”) of claims from three related patents directed to “[d]etermining the trustworthiness of information used to identify entities.” U.S. Patent No. 10,674,009 at 1:20–21 (the “’009 Patent”); U.S. Patent No. 11,005,989 at 1:23–24 (the “’989 Patent”); U.S. Patent No. 11,856,132 at 1:27–28 (the “’132 Patent”). The parties dispute the scope of two terms—“device fingerprint” and “performing a security determination.” Having considered the parties’ briefing, along with arguments of counsel at an April 30, 2025 hearing, the Court resolves the disputes as follows.

I. BACKGROUND

The patents, which are related and share the same disclosure,¹ concern device

¹ See ’132 Patent at [63] (setting forth the related application data and identifying the latter two applications as continuations of the first).

identification. The patents explain that “[d]etermining the trustworthiness of information used to identify entities involved in communications, such as text messages (e.g., SMS), email, calls, and instant messaging can be challenging.” ’009 Patent at 1:20–23. Caller ID and related technologies can be “spoofed,” making it difficult to trust caller identity information. *Id.* at 1:23–26. As a result, a malicious actor could, for example, call a bank’s customer while showing the bank’s number, thus convincing the customer that the call is legitimate and thereafter seek the customer’s account information and passwords.



FIGS. 2A (left) & 2B (right) of the '009 Patent, which show the steps taken by the mobile device and verification system, respectively, according to one embodiment.

To address the problem, the patents teach using a second communications channel—that is, a channel other than the channel on which the original communication was made—to transmit a message to the device associated with the phone number and then evaluate a response from that

device to decide whether the call is authentic. For example, as shown in Figures 2A and 2B (above), after a user initiates a call to a phone number associated with a device (steps 202, 204), the device receives a verification request from the system (steps 206, 224) over a different channel. The device then transmits a response to the system (step 208), which evaluates the response to make a security determination (step 230)—that is, to determine whether the call is, in fact, coming from the device associated with the phone number. If not, the system can block the call. *See generally* '009 Patent at 15:16–17:32.

Some embodiments contemplate enrolling devices in a system. After initial contact purportedly from a specific device, the system transmits a reply to the device that includes, for example, a numeric code or unique phrase. If the device transmits that code or phrase back to the system, the system concludes the device is, in fact, attempting to contact the system and that it is not a fraudulent attempt from a different source. After enrollment, any device information or unique identifiers set by the device are stored in the system and associated with the device for future use. *See generally* '009 Patent at 19:4–28.

Claim 1 of the '009 Patent is directed to such a system. Specifically, Claim 1 recites:

1. A system, comprising:
 - a verification service provider, configured to, using one or more processors:
 - enroll a first device with the verification service provider, wherein enrolling the first device includes associating, by the verification service provider, the first device with a **device fingerprint** that is generated based at least in part on a set of configuration information associated with the first device;
 - store, at the verification service provider, the **device fingerprint** associated with the first device;
 - obtain, at the verification service provider, information transmitted by a second device associated with a

communications connection;

perform, at the verification service provider, a security determination at least in part by determining whether the obtained information transmitted by the second device matches at least a portion of the stored **device fingerprint** that was generated based at least in part on the set of configuration information associated with the enrolled first device; and

based at least in part on the security determination, select an action comprising at least one of blocking the communication, requesting additional authentication, and permitting the communication.

'009 Patent at 22:47–23:4 (disputed terms in bold).

Other claims don't require "enrollment." For example, Claim 1 of the '989 Patent recites:

1. A system, comprising:

one or more processors configured to:

receive information pertaining to a call initiated by a calling device, the information pertaining to the call including: (1) a value generated based at least in part on information associated with the calling device, and (2) a score generated for the calling device, the score indicating a validity of a phone number;

perform a security determination based at least in part on the score generated for the calling device, and at least in part by verifying the value included in the information pertaining to the call initiated by the calling device; and

based at least in part on the security determination, perform at least one of conveying an assurance to a callee associated with the call or conveying a failure to confirm to the callee associated with the call; and

a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.

'989 Patent at 22:48–67 (disputed terms in bold).

The parties dispute the scope of two terms—"device fingerprint" and "performing a

security determination.” Regarding the former, the parties agree that “device fingerprint” refers to a “device identifier,” but they dispute whether it must be “unique.” As for the latter, Defendants assert that “performing a security determination” is a means-plus-function term without adequately disclosed structure, and therefore the claims reciting this term are indefinite.

II. LEGAL STANDARDS

A. Generally

“[T]he 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*). Accordingly, if the parties dispute the scope of the claims, the court must determine their meaning. *See, e.g., Verizon Servs. Corp. v. Vonage Holdings Corp.*, 503 F.3d 1295, 1317 (Fed. Cir. 2007) (Gajarsa, J., concurring in part); *see also Markman v. Westview Instruments, Inc.*, 517 U.S. 370, 390 (1996), *aff’g* 52 F.3d 967, 976 (Fed. Cir. 1995) (*en banc*).

Claim construction, however, “is not an obligatory exercise in redundancy.” *U.S. Surgical Corp. v. Ethicon, Inc.*, 103 F.3d 1554, 1568 (Fed. Cir. 1997). Rather, “[c]laim construction is a matter of [resolving] disputed meanings and technical scope, to clarify and when necessary to explain what the patentee covered by the claims” *Id.* A court need not “repeat or restate every claim term in order to comply with the ruling that claim construction is for the court.” *Id.*

When construing claims, “[t]here is a heavy presumption that claim terms are to be given their ordinary and customary meaning.” *Aventis Pharm. Inc. v. Amino Chems. Ltd.*, 715 F.3d 1363, 1373 (Fed. Cir. 2013) (citing *Phillips*, 415 F.3d at 1312–13). Courts must therefore “look to the words of the claims themselves . . . to define the scope of the patented invention.” *Id.* (citations omitted). The “ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, *i.e.*, as of the effective filing date of the patent application.” *Phillips*, 415 F.3d at 1313. This “person of ordinary

skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification.” *Id.*

Intrinsic evidence is the primary resource for claim construction. *See Power-One, Inc. v. Artesyn Techs., Inc.*, 599 F.3d 1343, 1348 (Fed. Cir. 2010) (citing *Phillips*, 415 F.3d at 1312). For certain claim terms, “the ordinary meaning of claim language as understood by a person of skill in the art may be readily apparent even to lay judges, and claim construction in such cases involves little more than the application of the widely accepted meaning of commonly understood words.” *Phillips*, 415 F.3d at 1314; *see also Medrad, Inc. v. MRI Devices Corp.*, 401 F.3d 1313, 1319 (Fed. Cir. 2005) (“We cannot look at the ordinary meaning of the term . . . in a vacuum. Rather, we must look at the ordinary meaning in the context of the written description and the prosecution history.”). But for claim terms with less-apparent meanings, courts consider “those sources available to the public that show what a person of skill in the art would have understood disputed claim language to mean . . . [including] the words of the claims themselves, the remainder of the specification, the prosecution history, and extrinsic evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art.” *Phillips*, 415 F.3d at 1314.

B. Means-Plus-Function Claiming²

A patent claim may be expressed using functional language. *See* 35 U.S.C. § 112(f); *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1347–49 & n.3 (Fed. Cir. 2015) (*en banc* in relevant portion). Under 35 U.S.C. § 112(f), a structure may be claimed as a “means . . . for performing a specified function,” and an act may be claimed as a “step for performing a specified

² Given the patents’ post-AIA effective filing dates, the Court will refer to 35 U.S.C. § 112(f), even though the cases cited in this section refer to the pre-AIA version of the statute.

function.” *Masco Corp. v. United States*, 303 F.3d 1316, 1326 (Fed. Cir. 2002). When it applies, § 112(f) limits the scope of the functional term “to only the structure, materials, or acts described in the specification as corresponding to the claimed function and equivalents thereof.” *Williamson*, 792 F.3d at 1347.

But § 112(f) does not apply to all functional claim language. There is a rebuttable presumption that § 112(f) applies when the claim language includes “means” or “step for” terms, and there is a rebuttable presumption that it does *not* apply in the absence of those terms. *Masco Corp.*, 303 F.3d at 1326; *Williamson*, 792 F.3d at 1348. These presumptions stand or fall according to whether one of ordinary skill in the art would understand the claim with the functional language to denote sufficiently definite structure or acts for performing the function in the context of the entire specification. *See Media Rights Techs., Inc. v. Capital One Fin. Corp.*, 800 F.3d 1366, 1372 (Fed. Cir. 2015) (noting that § 112(f) does not apply when “the claim language, read in light of the specification, recites sufficiently definite structure” (quotation marks omitted) (citing *Williamson*, 792 F.3d at 1349; *Robert Bosch, LLC v. Snap-On Inc.*, 769 F.3d 1094, 1099 (Fed. Cir. 2014))); *Masco Corp.*, 303 F.3d at 1326 (noting that § 112(f) does not apply when the claim includes an “act” corresponding to “how the function is performed”); *Personalized Media Commc’ns, LLC v. I.T.C.*, 161 F.3d 696, 704 (Fed. Cir. 1998) (noting that § 112(f) does not apply when the claim includes “sufficient structure, material, or acts within the claim itself to perform entirely the recited function . . . even if the claim uses the term ‘means.’” (quotation marks and citation omitted)).

Construing a means-plus-function limitation involves multiple steps. Step 1 “is a determination of the function of the means-plus-function limitation.” *Medtronic, Inc. v. Advanced Cardiovascular Sys., Inc.*, 248 F.3d 1303, 1311 (Fed. Cir. 2001). “[Step 2] is to determine the corresponding structure described in the specification and equivalents thereof.” *Id.* “Structure

disclosed in the specification is corresponding structure only if the specification or prosecution history clearly links or associates that structure to the function recited in the claim.” *Id.* (internal quotation marks omitted). The corresponding structure “must include all structure that actually performs the recited function.” *Default Proof Credit Card Sys. v. Home Depot U.S.A., Inc.*, 412 F.3d 1291, 1298 (Fed. Cir. 2005). But § 112(f) does not permit “incorporation of structure from the written description beyond that necessary to perform the claimed function.” *Micro Chem., Inc. v. Great Plains Chem. Co.*, 194 F.3d 1250, 1258 (Fed. Cir. 1999).

“[S]tructure can be recited in various ways, including [by using] ‘a claim term with a structural definition that is either provided in the specification or generally known in the art,’ or a description of the claim limitation’s operation and ‘how the function is achieved in the context of the invention.’” *Dyfan, LLC v. Target Corp.*, 28 F.4th 1360, 1366 (Fed. Cir. 2022) (quoting *Apple, Inc. v. Motorola, Inc.*, 757 F.3d 1286, 1299 (Fed. Cir. 2005)). For § 112(f) limitations implemented by a programmed general-purpose computer or microprocessor, the corresponding structure described in the patent specification must usually include an algorithm for performing the function. *WMS Gaming Inc. v. Int’l Game Tech.*, 184 F.3d 1339, 1349 (Fed. Cir. 1999). In that case, the corresponding structure is not a general-purpose computer but rather the special-purpose computer programmed to perform the disclosed algorithm. *Aristocrat Techs. Austl. Pty Ltd. v. Int’l Game Tech.*, 521 F.3d 1328, 1333 (Fed. Cir. 2008).

C. Indefiniteness

“[A] patent is invalid for indefiniteness if its claims, read in light of the specification delineating the patent, and the prosecution history, fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention.” *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 901 (2014). The claims “must be precise enough to afford clear notice of what is claimed” while recognizing that “some modicum of uncertainty” is inherent due to the limitations

of language. *Id.* at 908.

“Indefiniteness must be proven by clear and convincing evidence.” *Sonix Tech. Co. v. Publ’ns Int’l, Ltd.*, 844 F.3d 1370, 1377 (Fed. Cir. 2017). And in the context of § 112(f), “[t]he party alleging that the specification fails to disclose sufficient corresponding structure must make that showing by clear and convincing evidence.” *TecSec, Inc. v. IBM*, 731 F.3d 1336, 1349 (Fed. Cir. 2013) (quoting *Budde v. Harley-Davidson, Inc.*, 250 F.3d 1369, 1380–81 (Fed. Cir. 2001)).

III. THE LEVEL OF ORDINARY SKILL IN THE ART

The level of ordinary skill in the art is the skill level of a hypothetical person who is presumed to have known the relevant art at the time of the invention. *In re GPAC*, 57 F.3d 1573, 1579 (Fed. Cir. 1995). In resolving the appropriate level of ordinary skill, courts consider the types of and solutions to problems encountered in the art, the speed of innovation, the sophistication of the technology, and the education of workers active in the field. *Id.* Importantly, “[a] person of ordinary skill in the art is also a person of ordinary creativity, not an automaton.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 421 (2007).

Here, neither party addresses the level of ordinary skill in their briefing. RightQuestion’s expert, however, characterizes a skilled artisan as one with, at the time of invention, “an undergraduate degree in electrical engineering, computer science, computer engineering, or a related field, proficient in principals of computer security and the use of cryptography, and at least 2 years of experience in the development and testing of device authentication and security as implemented in network communications or telecommunications systems.” Malek Decl., Dkt. No. 57-8 ¶ 17. Defendants’ expert proffers a similar characterization. *See* Butler Decl., Dkt. No. 60-5 ¶ 33 (“[A] POSITA would have had at least a Bachelor’s degree in computer science, electrical engineering or a related technical field, and at least two years of professional experience, or an equivalent advanced education, in the field in security of cellular/telephony networks and mobile

systems.”). The Court sees no material differences between these levels of skill for the purpose of resolving these disputes, nor do the parties assert any such difference.

IV. THE DISPUTED TERMS

A. “device fingerprint” (’009 Patent, Claims 1, 9, 10, 17; ’989 Patent, Claims 12, 14)

Plaintiff’s Construction	Defendants’ Construction
“device identifier”	“unique device identifier”

Claims 1, 10, and 17 of the ’009 Patent recite “enroll[ing] a first device [a] verification service provider [by] associating, by the verification service provider, the first device with a device fingerprint that is generated based at least in part on a set of configuration information associated with the first device.” ’009 Patent at 22:50–55, 23:39–44, 24:24–29. The claims then require “stor[ing] at the verification service provider, the device fingerprint associated with the first device,” and “determining whether . . . obtained information transmitted by the second device matches at least a portion of the stored device fingerprint.” *Id.* at 22:56–57, 22:62–65, 23:39–46, 23:51–54; 24:30–31, 24:36–39.

The parties dispute the scope of “device fingerprint.” More specifically, although the parties agree that a “device fingerprint” is a “device identifier,” they dispute whether a “device fingerprint” must be “unique.” Defendants say it must, because “device identifier” is a well-known technical term that requires uniqueness, Dkt. No. 60 at 8 (citing papers), and the specification supports the notion of “uniqueness,” *id.* at 9 (citing ’009 Patent at 9:23–34). RightQuestion, however, says that “the specification is consistent in showing that the device fingerprint need *not* be unique.” Dkt. No. 57 at 6 (citing ’009 Patent at 9:23–24). Moreover, the specification uses “unique device identifier” separately, suggesting a distinction from “device fingerprint.” *Id.* at 8.

“Device fingerprint” appears in the specification twice. First, the patent explains that a

“verification service evaluates the device information and unique identifier to determine a match against previous usage of the device that is recorded and stored at the verification service.” ’009 Patent at 9:24–27. Then, “[e]xamples of device information include . . . a device ‘fingerprint’ created from a combination of device settings, installed applications, system or application software versions, or contact list stored on the phone.” *Id.* at 9:27–34. Elsewhere, the patent states that a device’s “fingerprint” could change if the device’s characteristics change. *See id.* at 9:55–10:1.

The Court agrees with Defendants. The lay meaning of “fingerprint” suggests uniqueness. Moreover, Defendants cite extrinsic evidence showing that “device fingerprint” is a well-known technical term” that contemplates uniqueness. Dkt. No. 60 at 8 (citing *Identifying Unique Devices Through Wireless Fingerprinting*, Dkt. No. 60-1 at 46 (“fingerprinting is a process by which a machine, driver, or the software the machine is running can be uniquely identified due to its externally observable characteristics”); *A Passive Approach to Wireless Device Fingerprinting*, Dkt. No. 60-2 at 383 (“Fingerprinting networked devices has been around for many years. The general idea is to extract leaked information about the device’s software, operating system, or hardware components” to “uniquely identify specific devices.”); *On Physical-Layer Identification of Wireless Devices*, Dkt. No. 60-3 at 6:1 (“Devices are traditionally identified by some unique information that they hold as a public identifier or a secret key. Besides what they hold, devices can be identified by what they are, that is, by some unique characteristics that they exhibit and that can be observed. . . . Analyzing these components for identifiable information is commonly referred to as fingerprinting, since the goal is to create fingerprints similar to their biometric counterparts.”)).

RightQuestion, however, disagrees with any “uniqueness” requirement. First, it points to

language from the specification that it says distinguishes between “device information” on one hand and “unique identifier” and “unique device identifier” on the other. *See* Dkt. No. 57 at 7 (quoting ’009 Patent at 9:23–24); *id.* at 8 (quoting ’009 Patent at 19:15–21). Consequently, says RightQuestion, “a device fingerprint is a type of device information and necessarily not a ‘unique identifier.’” But these are different things, with the “unique identifier” and “unique device identifier”³ being something like an arbitrarily assigned phrase or numeric code known only to the device and system. *See, e.g.,* ’009 Patent at 14:15–23 (describing the use of the phrase “purple cow” as a unique identifier known only to the device and the system); *id.* at 20:59–61 (“In various embodiments, the unique identifier includes one or more of a number, phrase, tone, or any other appropriate unique identifier.”). Accordingly, because it has nothing to do with “device information,” it provides little, if any, insight into the uniqueness of “device fingerprint.”

Moreover, to the extent the terms are comparable, RightQuestion presumes that difference must relate to “uniqueness.” Yet both could be “unique,” with a “device fingerprint” being one type of “unique device identifier,” and a public identifier or secret key as a different type of “unique device identifier” that does not depend on configuration information.

RightQuestion also points to the disclosure that a “device fingerprint” can be created from a combination of device settings, installed applications, system or application software versions, or a stored contact list—none of which are unique. It reasons that “[a] device fingerprint that is generated from information that is not unique, or is only semi-unique, is itself not necessarily unique.” Dkt. No. 57 at 7. While accurate, that argument ignores whatever meaning “fingerprint”

³ The specification refers to “unique device identifier” only once but uses the term interchangeably with “unique identifier.” *See* ’009 Patent at 19:19–22 (describing an embodiment in which “a network connection . . . deliver[s] a *unique device identifier* that is then stored (522) into local storage 512 by the verification service 510. The *unique identifier* is also stored locally at the smartphone device” (emphasis added)).

has in this context and incorrectly treats the “generated based on . . .” claim language as definitional rather than simply limiting.

Elsewhere, RightQuestion contends that if the patentee wanted to make the fingerprint unique it could have done so. Dkt. No. 57 at 8–9. This contention, however, ignores the meaning of “fingerprint” and instead presupposes the correctness of RightQuestion’s construction. After all, if Defendants are correct as to the meaning of the term, a “device fingerprint” is unique without any need to modify the term further.

Finally, RightQuestion criticizes Defendants’ reliance on extrinsic evidence as showing existing device fingerprinting techniques are imperfect. For example, RightQuestion stresses that one reference on which Defendants rely “achieved an average accuracy of about 70% to 80% in differentiating between unique devices.” Dkt. No. 65 at 2 (quoting *Identifying Unique Devices Through Wireless Fingerprinting*, Dkt. No. 60-1 at 54). Another approach achieved “uniqueness” only 40% to 60% of the time. *Id.* (citing *A Passive Approach to Wireless Device Fingerprinting*, Dkt. No. 60-2 at 391). Thus, while the goal might be perfect accuracy, RightQuestion says practically that goal is unachievable, which supports its construction. *Id.* at 2–4.

Here, too, the Court disagrees. That the *goal* might be perfect accuracy, even if that goal is practically unattainable, supports Defendants’ construction. That a technique might be less than perfect in creating a device fingerprint for all devices within a group shows a skilled artisan would understand a fingerprint to be unique. Otherwise, there would not be less-than-perfect accuracy. RightQuestion implicitly acknowledged as much during the hearing, noting “most of the time it works,” and the chances of “run[ning] into a collision, where you do have two phones with [an] identical device fingerprint” are “small.” Hr’g Tr., Dkt. No. 73 at 15:5–6, 15:9. Effectively, RightQuestion’s position amounts to reasoning “device fingerprint” should be construed based at

least in part on the practical difficulties of implementing the claimed system, which is not a claim-construction principle.

Moreover, to read the term as RightQuestion asks—that is, to not require device fingerprints to be unique—is not consistent with the notion that “most of the time it works” and it is only worried about cases on the margin. For example, if the set of configuration information on which the device fingerprint is based is *only* on system version information, which Claim 8 contemplates, every smartphone running the same system version would have the same “device fingerprint.” That would lead to far more than just isolated collisions.⁴

Accordingly, the Court adopts Defendants’ position and construes “device fingerprint” as “unique device identifier”⁵ but clarifies that “uniqueness” only relates to the claimed system. In other words, nothing suggests the “device fingerprint” must be unique *to the world*, nor is that required for the system to work. *See* Hr’g Tr., Dkt. No. 73 at 33:20–34:1 (agreement by Defendants that the scope of uniqueness “runs throughout the verification service provider but no further”). Moreover, the claim is open-ended, so that an accused system might generate both unique fingerprints and non-unique device information (e.g., when the “small” chance of a “collision” comes to fruition) does not appear to exclude that system from the scope of the claims.

⁴ RightQuestion says that this is acceptable because the last step of Claim 1 of the ’009 Patent provides for “requesting additional authentication.” Notably, however, Claim 1 does not *require* “requesting additional authentication,” as other options include blocking and permitting the communication. Moreover, nothing in the specification suggests that “requesting additional authentication” is tied to instances where less-than-unique device fingerprints are stored at the “verification service provider.” Instead, the specification links “requesting additional authentication” to creating a “verification score” by, for example, applying relative weighting to each available factor and then either blocking access, permitting access, or “requesting additional authentication” based on the value of that score. *See* ’009 Patent at 23:1–4.

⁵ As already noted, the specification uses “device identifier” and “unique device identifier” as a category of information different from “device information.” However, given that the parties submitted identical proposed constructions other than the word “unique,” the Court opts to stay within the confines of those proposals.

B. “perform[ing] a security determination” (’989 Patent, Claims 1, 27, 28; ’132 Patent, Claim 1)

Plaintiff’s Construction	Defendants’ Construction
Plain and ordinary meaning; not a means-plus-function or step-plus-function limitation.	Indefinite under 35 U.S.C. § 112(f)

This dispute concerns two apparatus claims and two method claims that each recite some version of “performing a security determination” based on one or more inputs received in a prior step. For example, Claim 1 of the ’989 Patent requires a processor configured to “perform a security determination based at least in part on the score generated for the calling device, and at least in part by verifying the value included in the information pertaining to the call initiated by the calling device.” ’989 Patent at 22:56–60; *see also id.* at 24:33–37 (reciting, in Claim 27, “performing a security determination” based on the same inputs); *id.* at 24:42–59 (reciting, in Claim 28, a computer instruction for “performing, at the verification service provider, a security determination”); ’132 Patent at 22:61–64 (reciting, in Claim 1, the step of “performing a security determination based at least in part on the cryptographic element associated with the caller device comprised in the received information pertaining to the call”).

Relying in part on *WSOU Invs. LLC v. Google LLC*, Nos. 2022-1063, 2022-1065, 2023 WL 6889033 (Fed. Cir. 2023), Defendants assert that these are means-plus-function terms without any clearly linked corresponding structure, and thus indefinite. They call the claim language “circular,” noting that “the processor [of Claims 1 and 28 of the ’989 Patent] receives a ‘score’ and ‘value’ and then runs some processes on that data.” Dkt. No. 60 at 13. In their view, “[t]he specification imparts no meaningful details on how the claimed processor is configured to perform a security determination.” *Id.* at 14.

RightQuestion counters with the well-known presumption against means-plus-function

treatment based on the lack of “means for” and “step for” language. Dkt. No. 57 at 11–12. And even if these are means-plus-function terms, RightQuestion says that the specification discloses adequate corresponding structure. *Id.* at 20–27. RightQuestion also points to *WSOU*, which held that a “processor configured to . . .” claim was not a means-plus-function term when the specification disclosed the processor as hardware. Dkt. No. 65 at 5–6.

These are not means- or step-plus-function limitations. First, the phrases at issue do not use “means for” or “step for” language, so the Court presumes that § 112(f) does not apply. Second, Defendants point to nothing in the claim language that might be considered a “nonce” term or otherwise as a generic description of structure or a step.⁶ Rather, they argue that the step as recited is not specific enough. *See, e.g.*, Dkt. No. 60 at 17 (“These are generic steps, and they do not provide any details on how the security determination is performed.”).

Regarding Claims 1 and 28 of the ’989 Patent, Defendants call the limitations “akin to the processor claim in *WSOU*,” Dkt. No. 60 at 14, but the Court disagrees. In *WSOU*, the appellate court considered the language “a processor configured” Affirming the district court’s conclusion of § 112 ¶ 6 treatment, the court relied on the specification’s broad disclosure of what a processor could be. *WSOU*, 2023 WL 6889033, at *4 (“In this case, as the district court correctly noted, the specification treats the word ‘processor’ so broadly as to generically be any structure that manipulates data.”). Defendants point to no such broad treatment of “processor” here.⁷

⁶ Defendants’ expert, however, considers the entirety of the preamble of Claim 28 of the ’989 Patent a nonce word. Butler Decl., Dkt. No. 60-5 ¶ 46.

⁷ Defendants do, however, point to a portion of the specification that explains the invention “can be implemented in numerous ways, including as a process; an apparatus; a system; a composition of matter; a computer program product embodied on a computer readable storage medium; and/or a processor, such as a processor configured to execute instructions stored on and/or provided by a memory coupled to the processor.” Dkt. No. 60 at 14–15 (quoting ’009 Patent at 2:8–25). At best, however, this boilerplate language concerns the invention as a whole rather than the “processor.” In contrast, the language at issue in *WSOU* referred to a specific embodiment and stated “[i]mplementation of the processor 4 can be in hardware alone (a circuit, a microprocessor etc, have certain aspects in

The claim language at issue here is closer to the other claim from *WSOU*, which recited:

1. An apparatus comprising:
at least one processor; and
***at least one memory including computer program code, where
the at least one memory and the computer program code
are configured, with the at least one processor, to cause the
apparatus to at least:***
[perform six specific steps].

Id. at *1–2 (quoting ’825 Patent at 10:29–61). For that claim, the court concluded that, “[t]hough terms like ‘computer program code,’ ‘memory,’ and ‘processor’ may be broad, the recited combination of these multiple broadly named structures informs the skilled artisan’s relative understanding of what each structure is and what it is not, as well as how the various structures relate to one another.” *Id.* at *4. Similarly, the processor claim here recites “one or more processors” and “memory coupled to the one or more processors and configured to provide the one or more processors with instructions.” ’989 Patent at 22:49, 22:65–67.

Apple Inc. v. Motorola, Inc., 757 F.3d 1286 (Fed. Cir. 2014), is also instructive. In *Apple*, the patents at issue recited limitations directed to “heuristics.” For example, one patent recited:

- a vertical screen scrolling heuristic* for determining that the one or more finger contacts correspond to a one-dimensional vertical screen scrolling command rather than a two-dimensional screen translation command *based on an angle of initial movement of a finger contact with respect to the touch screen display*; [and]
- a two-dimensional screen translation heuristic* for determining that the one or more finger contacts correspond to the two-dimensional screen translation command rather than the one-dimensional vertical screen scrolling command *based on the angle of initial movement of the finger contact with respect to*

software including firmware alone or can be a combination of hardware and software (including firmware).” *See WSOU*, 2023 WL 6889033, at *9 (quoting ’045 Patent at 13:6–9, 14:7–21).

the touch screen display[.]

Apple, 757 F.3d at 1295 (quoting Claim 1 of U.S. Patent 7,479,949). Considering whether these were means-plus-function limitations, the court explained:

“Structure” to a person of ordinary skill in the art of computer-implemented inventions may differ from more traditional, mechanical structure. For example, looking for traditional “physical structure” in a computer software claim is fruitless because software does not contain physical structures. Indeed, the typical physical structure that implements software, a computer, cannot be relied upon to provide sufficiently definite structure for a software claim lacking “means.” Rather, to one of skill in the art, the “structure” of computer software is understood through, for example, an outline of an algorithm, a flowchart, or a specific set of instructions or rules. *See, e.g., Typhoon Touch*, 659 F.3d at 1385 (“[T]he patent need only disclose sufficient structure for a person of skill in the field to provide an operative software program for the specified function.”)

Apple, 757 F.3d at 1298–99. Ultimately, the court concluded these “heuristic” limitations were “sufficiently definite structure” to avoid means-plus-function treatment because “the claims do not nakedly recite heuristics without further description in the remaining claim language and specification. To the contrary, the claim language and specification disclose the heuristics’ operation within the context of the invention, including the inputs, outputs, and how certain outputs are achieved.” *Id.* at 1301. The court found “that ‘heuristic’ has a known meaning and the ’949 patent also describes the limitation’s operation, including its input, output, and how its output may be achieved. Accordingly, the heuristic claim limitations recited above have ‘sufficiently definite structure,’ to a person of ordinary skill in the art, for performing the recited functions.” *Id.* at 1300.

The same reasoning applies here. “Processor” and “instruction” have known meanings, and like the limitations at issue in *Apple*, the various “performing a security determination” steps or instructions are “based on” some input received in a previous step—either (1) the score indicating a validity of the phone number and a value generated based on device information, or (2) a cryptographic element. The specification discloses the “security determination” is a binary

outcome as to whether the device is authenticated. *See* '989 Patent at 17:22–39 (referring to positive and negative security determinations). The specification also shows that making a “security determination” is simply validating the received information or determining whether the received score exceeds some threshold. For example, if a response from a device corresponds to a message transmitted to the device, “then a positive security determination is made. If an invalid response is received, or no response at all is received, for example, within a threshold amount of time, then a negative security determination is made.” *Id.* at 17:22–26. The patent also explains that the relying party can specify the required score for verification. *Id.* at 10:6–8 (“In some embodiments, the relying party specifies, to the verification service, the score that is required to complete a verification.”); *see also id.* at 9:55–58 (explaining the “verification score” must be sufficient or the verification server will contact the device a second time). Regarding the cryptographic element, the specification explains that the element is stored at both the user device and the verification service provider and used to validate the device. A skilled artisan would understand this to require determining whether the received cryptographic element matches the cryptographic element associated with the device at the system. Collectively, these disclosures provide sufficiently definite structure to avoid invoking § 112(f).

Notably, neither Defendants nor their expert provide much consideration of the specification when determining whether the limitations connote “sufficiently definite structure.” Generally, however, Defendants assert that the patents “simply tell the skilled artisan to use a processor to perform the function.” Dkt. No. 60 at 18. The Court disagrees because, as noted above, the specification provides enough for a skilled artisan to understand the scope of “performing a security determination” based on the inputs recited in the respective claims, the output, and the specifications’ description of how the inventions work. Accordingly, the “performing a security

determination” limitations provide “sufficiently definite structure” to a skilled artisan⁸ and, because these are not § 112(f) terms, the Court will give them “plain and ordinary meaning” constructions.

V. CONCLUSION

Disputed Term	The Court’s Construction
“device fingerprint” (’009 Patent, Claims 1, 9, 10, 17; ’989 Patent, Claims 12, 14)	“unique device identifier”
“perform[ing] a security determination” (’989 Patent, Claims 1, 27, 28; ’132 Patent, Claim 1)	Plain and ordinary meaning

The Court **ORDERS** each party not to refer, directly or indirectly, to its own or any other party’s claim-construction positions in the presence of the jury. Likewise, the Court **ORDERS** the parties to refrain from mentioning any part of this opinion, other than the actual positions adopted by the Court, in the presence of the jury. Neither party may take a position before the jury that contradicts the Court’s reasoning in this opinion. Any reference to claim construction proceedings is limited to informing the jury of the positions adopted by the Court.

So ORDERED and SIGNED this 30th day of May, 2025.



RODNEY GILSTRAP
UNITED STATES DISTRICT JUDGE

⁸ Even if the Court were to hold these are means-plus-function limitations, the Court would not hold they are indefinite for lack of corresponding structure given these disclosures.