

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION**

PROXENSE, LLC,

Plaintiff,

v.

MICROSOFT CORPORATION,

Defendant.

Case No. 6:23-cv-00319-ADA



MICROSOFT CORPORATION'S MOTIONS FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. THE ASSERTED PATENT	2
III. LEGAL STANDARD.....	6
IV. MOTION #1: NO DIRECT INFRINGEMENT	7
A. There Is No Dispute of Material Fact with Respect to Dr. Rubin’s Infringement Theory	8
B. Microsoft Is Entitled to Judgment as a Matter of Law that It Does Not Directly Infringe the Claimed Method.....	9
1. The User of the Windows Device Are the Accused Direct Infringers as They Perform the Accused Method	9
2. Dr. Rubin’s Infringement Theory Requires Hardware but He Only Accuses Microsoft Software	10
3. Proxense Does Not Argue Any Divided Infringement Theory	11
V. MOTION #2: SUMMARY JUDGMENT THAT THE ACCUSED PRODUCTS DO NOT INFRINGE BECAUSE THEY LACK A “THIRD PARTY THAT OPERATES A TRUSTED AUTHORITY”	12
A. There Is No Genuine Dispute of Material Fact.....	13
B. Microsoft is Entitled to Summary Judgment: Microsoft Cannot be a “Third Party” to Itself.	15
1. The Intrinsic Evidence Does Not Support the Interpretation of “Third Party” as a Separate Server or Software System Still Belonging to the Same Company	15
a. The Specification of the ’954 Patent Does Not Support Dr. Rubin’s Implicit Construction	16
b. The ’954 Patent Provisional Applications Do Not Support a Broad Reading of Third Party.....	17
c. The Prosecution History Does Not Support Dr. Rubin’s New Broad Construction.....	19
d. Proxense’s Statements Made During the IPRs Contradict Dr. Rubin’s Implicit Construction.....	20
2. Dr. Rubin’s Argument About a Third Party Being Merely Separate Conflicts with His Other Opinions on Infringement and Validity.....	23

VI.	MOTION #3: SUMMARY JUDGMENT THAT THE ACCUSED PRODUCTS DO NOT INFRINGE BECAUSE THEY LACK “PERSISTENTLY STORING . . . IN A TAMPER PROOF FORMAT WRITTEN TO A STORAGE ELEMENT ON THE INTEGRATED DEVICE THAT IS NOT CAPABLE OF BEING SUBSEQUENTLY ALTERED”.....	23
VII.	MOTION #4: SUMMARY JUDGMENT THAT THE CLAIMS ARE INVALID UNDER § 101.....	27
A.	<i>Alice</i> Step One: The ’954 Patent Claims Are Directed to an Abstract Idea	27
B.	<i>Alice</i> Step Two: The ’954 Patent Claims Lack an Inventive Concept.....	31
C.	Representative Claim Analysis	33
VIII.	MOTION #5: THERE ARE NO GENUINE ISSUES OF MATERIAL FACT REGARDING THE LACK OF WILLFUL INFRINGEMENT.....	33
A.	Factual Background	33
B.	Legal Standard – Willful Infringement.....	34
C.	Proxense’s Claim for Pre-Suit Willfulness Fails Because It Has Not Shown that Microsoft Had Pre-Suit Knowledge of the ’954 Patent	35
D.	Proxense’s Post-Suit Willfulness Claim Also Fails Because Proxense Has Identified No Evidence of Intent to Infringe.....	38
IX.	CONCLUSION.....	40

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Alice Corp. Ltd. v. CLS Bank International</i> , 573 U.S. 208 (2014).....	27, 31, 32
<i>Anderson v. Liberty Lobby, Inc.</i> , 477 U.S. 242 (1986).....	6, 7
<i>Aylus Networks, Inc. v. Apple Inc.</i> , 856 F.3d 1353 (Fed. Cir. 2017).....	21
<i>BASF Plant Sci., LP v. Commonwealth Sci. & Indus. Research Org.</i> , 28 F.4th 1247 (Fed. Cir. 2022)	34
<i>Bayer Healthcare LLC v. Baxalta Inc.</i> , 989 F.3d 964 (Fed. Cir. 2021).....	34, 35
<i>Bioverativ Inc. v. CSL Behring LLC</i> , C.A. 17-914-RGA, 2020 WL 1332921 (D. Del. Mar. 23, 2020).....	40
<i>Boston Scientific Corp. v. Nevro Corp.</i> , 560 F. Supp. 3d 837 (D. Del. 2021).....	34
<i>BSG Tech LLC v. Buyseasons, Inc.</i> , 899 F.3d 1281 (Fed. Cir. 2018).....	32
<i>Celotex Corp. v. Catrett</i> , 477 U.S. 317 (1986).....	6, 7, 34
<i>Chamberlain Group, Inc. v. Techtronic Industries Co.</i> , 935 F.3d 1341 (Fed. Cir. 2019).....	31, 32
<i>CUPP Computing AS v. Trend Micro Inc.</i> , 53 F.4th 1376 (Fed. Cir. 2022)	21
<i>Electric Power Group, LLC v. Alstom S.A.</i> , 830 F.3d 1350 (Fed. Cir. 2016).....	29, 30, 31
<i>Ericsson, Inc. v. D-Link Sys., Inc.</i> , 773 F.3d 1201 (Fed. Cir. 2014).....	7, 9
<i>ESW Holdings v. Roku</i> , 6-19-CV-00044-ADA, 2021 WL 1069047 (W.D. Tex. March 18, 2021) (Albright, J.).....	12

<i>Evolved Wireless, LLC v. Apple Inc.</i> , C.A. No. 15-542-JFB-SRF, 2019 WL 8128550 (D. Del. Feb. 19, 2019)	39
<i>Google, LLC v. Proxense, LLC</i> , IPR2023-00232, Paper 10 (PTAB Jul. 24, 2024)	22
<i>Google, LLC v. Proxense, LLC</i> , IPR2024-00233, Paper 10 (PTAB Jul. 24, 2024)	22
<i>Google, LLC v. Proxense, LLC</i> , IPR2024-00234, Paper 10 (PTAB Jul. 24, 2024)	22
<i>Gustafson, Inc. v. Intersystems Indus. Prods., Inc.</i> , 897 F.2d 508 (Fed. Cir. 1990)	38
<i>Halo Elecs., Inc. v. Pulse Elecs., Inc.</i> , 579 U.S. 93 (2016)	35, 39, 40
<i>HOYA Corp. v. Alcon Inc.</i> , 713 F. Supp. 3d 291 (N.D. Tex. 2024)	35, 39
<i>i4i Ltd. P'ship v. Microsoft Corp.</i> , 598 F.3d 831 (Fed. Cir. 2010), <i>aff'd</i> , 564 U.S. 91 (2011)	<i>passim</i>
<i>Info. Images, LLC v. PGA TOUR, Inc.</i> , 686 F. Supp. 3d 549 (W.D. Tex. 2023), appeal dismissed, No. 2023-2362, 2023 WL 6784362 (Fed. Cir. Oct. 13, 2023) (Albright, J.)	12
<i>Int'l Bus. Machines Corp. v. Booking Holdings Inc.</i> , 775 F. App'x 674 (Fed. Cir. 2019)	7
<i>Intell. Ventures I LLC v. Symantec Corp.</i> , 838 F.3d 1307 (Fed. Cir. 2016)	27
<i>Koninklijke Philips N.V. v. Zoll Med. Corp.</i> , 656 F. App'x 504 (Fed. Cir. 2016)	9
<i>Lucent Techs., Inc. v. Gateway, Inc.</i> , 580 F.3d 1301 (Fed. Cir. 2009)	7
<i>M&C Innovations, LLC v. Igloo Prods. Corp.</i> , No. 4:17-CV-2372, 2018 WL 4620713 (S.D. Tex. July 31, 2018)	40
<i>Mobile Acuity Ltd., v. Blippar Ltd.</i> , 110 F.4th 1280 (Fed. Cir. 2024)	33
<i>NexStep, Inc. v. Comcast Cable Comm's, LLC</i> , No. 19-1031-RGA-SRF, 2021 WL 4077778 (D. Del. Aug. 20, 2021)	40

<i>Novartis Corp. v. Ben Venue Labs., Inc.</i> , 271 F.3d 1043 (Fed. Cir. 2001).....	6, 34
<i>Prism Techs. LLC v. T-Mobile USA, Inc.</i> , 696 F. App'x 1014 (Fed. Cir. 2017)	31, 32
<i>Proxense LLC v. Samsung Co, Ltd.</i> , No. 6:21-cv-00210-ADA (W.D. Tex. Dec. 28, 2022), Dkt. No. 149 (Ex. 32)	26
<i>Proxense, LLC v. Google LLC</i> , 6:23-cv-00320-ADA (W.D. Tex Nov. 26, 2024), Dkt. 120 (Ex. 11)	19
<i>Ravgen, Inc. v. Quest Diagnostics Inc.</i> , No. 2:21-cv-09011-RGK-GJS, 2022 WL 2047613 (C.D. Cal. Jan. 18, 2022)	40
<i>Ricoh Co. v. Quanta Computer Inc.</i> , 550 F.3d 1325 (Fed. Cir. 2008).....	9, 10
<i>Samsung Electronics America, Inc. v. Proxense, LLC</i> , IPR2021-01444, Paper 11 (PTAB Feb. 28, 2022)	21
<i>Samsung Electronics America, Inc. v. Proxense, LLC</i> , IPR2021-01447, Paper 12 (PTAB Feb. 28, 2022)	22
<i>Samsung Electronics America, Inc. v. Proxense, LLC</i> , IPR2021-01448, Paper 12 (PTAB Feb. 28, 2022)	22
<i>SRI Int'l, Inc. v. Cisco Sys., Inc.</i> , 14 F.4th 1323 (Fed. Cir. 2021), cert. denied, 142 S. Ct. 2732 (2022)	34, 39
<i>Synchronoss Techs., Inc. v. Dropbox, Inc.</i> , 987 F.3d 1358 (Fed. Cir. 2021).....	10
<i>Ultramercial, Inc. v. Hulu, LLC</i> , 772 F.3d 709 (Fed. Cir. 2014).....	32
<i>Universal Secure Registry LLC v. Apple Inc.</i> , 10 F.4th 1342 (Fed. Cir. 2021)	28, 29
<i>WesternGeco L.L.C. v. ION Geophysical Corp.</i> , 837 F.3d 1358 (Fed. Cir. 2016).....	2, 39

Statutes

35 U.S.C. § 101	1, 27, 29, 31
-----------------------	---------------

Other Authorities

Fed. R. Civ. P. 56(c)	6
-----------------------------	---

I. INTRODUCTION

Microsoft moves for summary judgment on five issues.

No Infringement. The three noninfringement issues relate to Proxense’s disregard for the express claim language of the sole remaining patent and basic legal principles. Specifically, Proxense points to Microsoft as being the direct infringer without any regard for the fact that its theory relies on actions of *users* of Microsoft Windows. For example, Proxense’s expert Dr. Rubin asserts that the claimed method is performed when a “Windows device utilized by the Microsoft user [wirelessly sends data] to Microsoft’s identity provider (IdP) server.” Dr. Rubin’s theory creates two major infringement issues for Proxense. *First*, the “user” by way of their Windows device is the accused direct infringer of the method claim, not Microsoft. It is elementary patent law that a method claim is infringed when performed. *Second*, Dr. Rubin explicitly accuses communicating data to a Microsoft server for a user of Microsoft applications. Accordingly, there is no “third party” in this process which is a required element of all asserted claims. *Finally*, Dr. Rubin also ignores the claims’ express requirement for data “not capable of being subsequently altered” and only argues that the accused data is encrypted. Not only did Proxense not request claim constructions to alter “third party” and “not capable of being subsequently altered,” Dr. Rubin’s arguments for both terms were explicitly disavowed in the patent’s prosecution history.

Invalidity. Microsoft also moves for invalidity under 35 U.S.C. § 101. The asserted claims are directed at the abstract idea of authenticating with a user’s biological characteristics (“characteristics unique to the user’s body” such as a fingerprint) *and* authenticating a physical object they possess with a third party. Proxense’s own expert analogizes the patent’s teachings to a “punch card issued by a coffee shop” to get “a free latte.” Additionally, for the “third party” authentication limitation that Proxense repeatedly invokes to try to overcome prior art by disavowing Dr. Rubin’s infringement theory, the specification contemplates authentication body

performed by “a government official, a notary, and/or an employee of a third party.” Finally, the patent lacks an inventive concept as it teaches use of conventional computer components such as the read only memory (ROM) which is “not capable of being subsequently altered” and which Dr. Rubin fails to show is in the accused devices.

No Willful Infringement. To the extent that the Court needs to reach this issue, Microsoft is entitled to summary judgment on Proxense’s willful infringement allegation. Proxense fails to show that Microsoft deliberately or intentionally infringes either before or after Proxense filed its Complaint. Before the Complaint, Proxense only alleges general knowledge of Proxense’s patent portfolio. This is insufficient as a matter of law. As for after the Complaint, Proxense does not allege any facts to show deliberate or intentional infringement given Microsoft’s objectively reasonable bases for its noninfringement (discussed herein) and invalidity defenses. Indeed, Microsoft has a good faith basis to believe that the ’954 patent is invalid at least because the PTAB granted institution of Microsoft’s—as well as Apple’s and Google’s—*inter partes* review petitions of the ’954 patent. All such facts support Microsoft’s post-complaint subjective belief that it does not infringe the ’954 patent. *WesternGeco L.L.C. v. ION Geophysical Corp.*, 837 F.3d 1358, 1363 (Fed. Cir. 2016).

II. THE ASSERTED PATENT

Only one patent remains asserted against Microsoft, Proxense having abandoned the other five. The remaining patent, U.S. Patent No. 8,886,954 (“’954 patent”) is titled “Biometric personal data key (PDK) authentication” and claims priority to U.S. Patent No. 8,352,730 (“’730 patent”).¹ These patents also claim priority to two provisional applications the earliest of which is a

¹ Proxense has already conceded unpatentability of all claims of the ’730 patent and acknowledges the asserted claims of this patent should be dismissed. The parties disagree only to whether all the claims of the ’730 patent should be dismissed with prejudice.

provisional U.S. Provisional Application No. 60/637,538 (“538 provisional”) which was filed on Dec. 20, 2004.

The ’954 patent background section explains that “[c]onventional user authentication techniques are designed to prevent access by unauthorized users” and “[o]ne technique is to require a user being authenticated to provide secret credentials, such as a password, before allowing access.” Ex. 1, ’954 patent at 1:26-29. However, with this method “[a] uses [sic] often has multiple sets of credentials (e.g., passwords and PINs) and it can be quite difficult to keep track of them all.” *Id.* at 1:33-35. The patent also recognizes that “[a]nother technique that does not require the user to memorize credentials is to provide the user with an access object such as a key (e.g., an electronic key) that the user can present to obtain access.” *Id.* at 1:36-39. The ’954 patent explains that “[a] difficulty with using access objects is that authentication merely proves that the access object itself is valid; it does not verify that the legitimate user is using the access object.” *Id.* at 1:41-44. Finally, the ’954 patent acknowledges that “[s]ome hybrid authentication techniques require the user to provide both an access object and credentials [but] this solution does not resolve the problem of making the user memorize credentials.” *Id.* at 1:47-51.

To solve these problems with existing hybrid authentication, the ’954 patent describes “systems and methods for authentication responsive to biometric verification of a user being authenticated.” *Id.* at 1:60-62. The alleged invention includes an integrated device that includes a biometric key that can “request a fingerprint scan from a user . . . when biometric verification is needed for the particular use.” *Id.* at 4:36-39. The ’954 patent does not teach any new biometric verification techniques. Instead, the ’954 patent describes that “[c]onventional techniques for comparing fingerprints can be used.” *Id.* at 5:11-13. According to the ’954 patent, if “scan data matches the biometric data, wirelessly sending a code for authentication.” *Id.* at 2:1-3. Figure 1

(below) illustrates an example biometric key. After authentication is successful, the user can access an application. *Id.* at Abstract. In the '954 patent, an application “is a resource that can be accessed by a verified and authenticated user” such as “a casino machine, a keyless lock, a garage door opener, [and] an ATM machine.” *Id.* at 6:18-21.

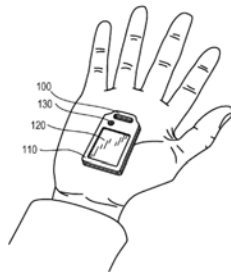


FIG. 1

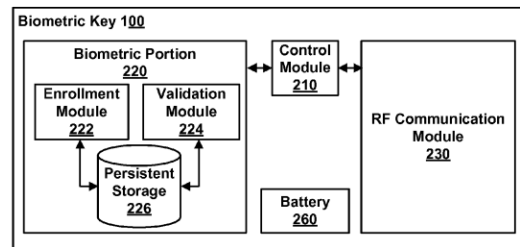


FIG. 2

The '954 patent also describes that the “integrated device includes a persistent storage to persistently stores [sic] a code such as a device identifier and biometric data for a user in a tamper-resistant format.” *Id.* at 1:62–2-2:3. “[A]t least some of persistent storage [] is a memory element that can be written to once but cannot subsequently be altered.” *Id.* at 5:24-26. According to the '954 patent, persistent storage “can include, for example, a ROM element,” or “read-only memories (ROMs).” *Id.* at 5:26-29, 9:34. Persistent storage is also “stored in a tamper-proof format to prevent any changes to the stored data.” *Id.* at 5:31-32. “Furthermore, data can be stored in an encrypted form.” *Id.* at 5:34-35.

As noted above, the persistent storage includes a “code such as a device identifier” which the patent also calls a “device ID or other value that uniquely identifies biometric key.” *Id.* at 5:38-40. The code may be “provid[ed] during the manufacturing process.” *Id.* at 5:40-41. To accomplish authentication, the '954 patent describes that the biometric key is wirelessly coupled to an authentication module. *See id.* at 6:1-5; *id.* at Fig. 3. After biometric verification, the authentication module “provides the code to trusted key authority 320 in order to verify that it belongs to a legitimate key (e.g., when application 330 is security-critical).” *Id.* at 6:11-14.

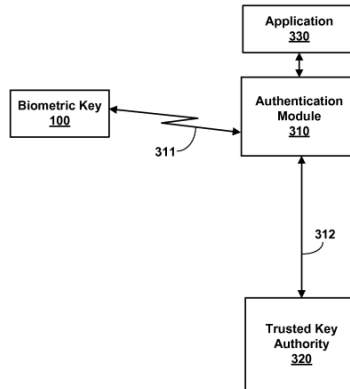


FIG. 3

The “[t]rusted key authority []” is a third-party authority that is present in some embodiments in order to provide enhanced security.” *Id.* at 6:35-37. The ’954 explains that for these types of systems the “code [that] uniquely identifies the integrated device” “is registered with a trusted authority, and the code can be authenticated to a third party by the trusted authority.” *Id.* at 2:26-34. The ’954 patent describes that to enroll “[a]n agent checks [] an identification of the user and establishes a profile.” *Id.* at 7:29-30. The ’954 patent explains that “[t]he agent can be, for example, a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness.” *Id.* at 7:30-33. Thereafter, “the trusted key authority [] stores a list of codes for legitimate biometric keys” so that it can verify that a code from the biometric key is legitimate. *Id.* at 6:37-40. The ’954 patent describes that data can then be sent to the “agent for authentication” and that the agent can send back an “access message” “indicating that the agent successfully authenticated the one or more codes and other data values and allows the user to access an application.” *Id.* at Abstract.

Claim 1, which is the only remaining independent claim, is below:

1. A method comprising:

persistently storing biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and

a secret decryption value in a tamper proof format written to a storage element on the integrated device that is ***not capable of being subsequently altered***;

responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

responsive to a determination that the scan data matches the biometric data, wirelessly ***sending one or more codes*** and other values from the plurality of codes and other data values ***for authentication to a third party that operates a trusted authority***, wherein the one or more codes and other data values includes the device ID code; and

receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party and allowing the user access to the application.

Ex. 1, '954 patent at 10:5-27 (emphasis added).

III. LEGAL STANDARD

Summary judgment is appropriate when, viewing the facts most favorably to the nonmoving party, there are no genuine issues of material fact and the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(c); *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 247-48 (1986); *see also Novartis Corp. v. Ben Venue Labs., Inc.*, 271 F.3d 1043, 1046 (Fed. Cir. 2001) (in the patent context, summary judgment of non-infringement may only be granted if “there is no genuine issue whether the accused device is encompassed by the [patent] claims.”). The movant bears the initial burden of showing the absence of any genuine issues of material fact. *Celotex Corp. v. Catrett*, 477 U.S. 317, 322-24 (1986). “[T]he plain language of Rule 56(c) mandates the entry of summary judgment, after adequate time for discovery and upon motion, against a party who fails to make a showing sufficient to establish the existence of an element essential to that party’s case, and on which that party will bear the burden of proof at trial.” *Id.* at 322. “In such a situation, there can be ‘no genuine issue as to any material fact,’ since complete

failure of proof concerning an essential element of the nonmoving party's case necessarily renders all other facts immaterial." *Id.* at 322-23. If the movant makes a prima facie case for summary judgment, the burden shifts to the nonmovant to present specific evidence raising a genuine issue for trial. *Anderson*, 477 U.S. at 250.

IV. MOTION #1: NO DIRECT INFRINGEMENT

The only remaining asserted claims are method claims directed at "biometric verification of the user" and an "integrated device." "To infringe a method claim, a person must have practiced all steps of the claimed method." *Lucent Techs., Inc. v. Gateway, Inc.*, 580 F.3d 1301, 1317 (Fed. Cir. 2009) (affirming a finding of direct infringement by Windows users of a "[a] method for use in a computer" claim and affirming that Microsoft was liable via *indirect* infringement).

Proxense's technical expert Dr. Rubin alleges that "[t]he 'integrated device' in Microsoft's implementation refers to the Windows 10 / 11 device utilized **by a Microsoft user when signing in** with Windows Hello to the Windows 10 / 11 device, a Microsoft Account, or a Microsoft 365 product or subscription." Ex. 2, Rubin Op. Rep. ¶ 103, Rubin Op. Rep. ¶ 324. It is settled law that the direct infringer of similar method claims which are directed at the use of a device is the user, not the party that sells the device. *See Ericsson, Inc. v. D-Link Sys., Inc.*, 773 F.3d 1201, 1222 (Fed. Cir. 2014) ("[N]one of our decisions have found direct infringement of a method claim by sales of an end user product which performs the entire method, and we decline to do so here."); *Int'l Bus. Machines Corp. v. Booking Holdings Inc.*, 775 F. App'x 674, 678 (Fed. Cir. 2019) ("[T]he district court properly granted summary judgment of noninfringement. There is no dispute that the storing step occurs on the users' device."). Therefore, Microsoft is entitled to summary judgment that it is not liable as a direct infringer.

A. There Is No Dispute of Material Fact with Respect to Dr. Rubin’s Infringement Theory

Dr. Rubin only identifies Microsoft’s software products (Windows 10, Windows 11, Office 365, and Microsoft 365). Ex. 2, Rubin Op. Rep. ¶ 1. However, Dr. Rubin’s infringement theory first requires a user to have a “Windows *device*” with certain hardware. Ex. 3, Rubin Dep. 39:22–40:5, 52:16-20; 169:19-24; Ex. 2, Rubin Op. Rep. ¶ 321 (“use of passwordless authentication with biometrics to access Windows 10 /11 devices”); ¶ 324 (“the user’s Windows device to be the integrated device”). Dr. Rubin’s opinion is that the claimed method is performed “[w]hen a Microsoft user signs in” to their device a certain way. *See, e.g.*, Ex. 2, Rubin Op. Rep. ¶ 165.

For example, Dr. Rubin’s opinion is only directed at users that log in to an account on a device that authenticates the user via Microsoft cloud authentication services. *Id.*, Rubin Op. Rep. ¶ 124 (discussing users signing into their device by “authenticating to the cloud”); Ex. 3, Rubin Dep. 190:2-6 (device must be registered to a server). Specifically, Dr. Rubin accuses accounts that authenticate with “Microsoft’s identity provider server Entra ID.”² Ex. 2, Rubin Op. Rep. ¶ 332; Ex. 3, Rubin Dep. 171:6-172:3 (admitting that he does not accuse accounts that do not communicate with a server of infringing). Dr. Rubin’s theory also requires users to log in via a biometric sensor (such as fingerprint scanner) with a Windows component called Windows Hello.³ Ex. 3, Rubin Dep. 169:1-24 (admitting he does not accuse device that are not capable of running Windows Hello); 190:15-18 (admitting that the device needs to be set up for “biometrics for log on to their Windows device”). That is not all, as Dr. Rubin’s theory only accuses the subset of logins made over a “wireless network.” *Id.*, Rubin Dep. 39:22-40:5, 190:7-13.

³ Microsoft uses “Windows Hello” to refer to both “Windows Hello” and “Windows Hello for Business” for the purposes of this motion. *See* Ex. 2, Rubin Op. Rep. ¶ 42.

There is no dispute of material fact as to Dr. Rubin's basic theory. The legal question is whether Microsoft can be liable for *direct* infringement based on this theory. Dr. Rubin admits that it is a legal question as to whether Microsoft selling software is infringement of a method claim. Ex. 3, Rubin Dep. 192:22-193:7 ("A. The act of selling the Windows? Your question is if that's performing the infringement? Q. Yes. . . . [A.] It sounds to me like that's more of a legal question than a technical one.").

B. Microsoft Is Entitled to Judgment as a Matter of Law that It Does Not Directly Infringe the Claimed Method

As to the legal question whether Microsoft is a direct infringer under Dr. Rubin's theory, the answer is clear. Microsoft is not a direct infringer as a matter of law because: (1) Microsoft's sale of software does perform the accused method steps on a user device, (2) Microsoft's sale of software does not include hardware and requires additional user configuration, and (3) Proxense does not allege any joint infringement theory or contend that Microsoft directs or controls its users to perform the method.

1. The User of the Windows Device Are the Accused Direct Infringers as They Perform the Accused Method

"[A] party that sells or offers to sell software containing *instructions to perform a patented method* does not infringe the patent under § 271(a)." *Ricoh Co. v. Quanta Computer Inc.*, 550 F.3d 1325, 1335 (Fed. Cir. 2008); *see Ericsson*, 773 F.3d at 1222; *i4i Ltd. P'ship v. Microsoft Corp.*, 598 F.3d 831, 850 (Fed. Cir. 2010), *aff'd*, 564 U.S. 91 (2011); *Koninklijke Philips N.V. v. Zoll Med. Corp.*, 656 F. App'x 504, 521 (Fed. Cir. 2016) ("all of the steps of the self-test method claims are performed by the defibrillator devices, wholly out of the control of Zoll.")

Here, the asserted claims are method claims where the steps are allegedly performed at the user's Window's device, the alleged "integrated device." Ex. 1, '954 patent at claim 1 ("persistently storing . . . on the integrated device. . . ; responsive to receiving a request for a

biometric verification of the user, receiving scan data from a biometric scan; comparing the scan data . . . ; responsive to a determination that the scan data matches the biometric data, wirelessly sending . . . to a third party . . . ; and receiving, at an application, an access message . . . allowing the user access to the application.”). Indeed, Dr. Rubin frequently cites the “user’s Windows device” to describe his theory. *See, e.g.*, Ex. 2, Rubin Op. Rep. ¶¶ 324, 334, 337.

Therefore, the sale of Microsoft software (which Dr. Rubin accuses and Dr. Cole and Dr. Vanderhart use for calculating damages) cannot be *direct* infringement. *See Ricoh*, 550 F.3d at 1335. Microsoft is entitled to summary judgment of no direct infringement.

2. Dr. Rubin’s Infringement Theory Requires Hardware but He Only Accuses Microsoft Software

The Federal Circuit confirmed that a party cannot be liable for direct infringement when “hardware” is involved in claim scope and the accused infringer only provides accused software. *See Synchronoss Techs., Inc. v. Dropbox, Inc.*, 987 F.3d 1358, 1368 (Fed. Cir. 2021). In *Synchronoss Techs.*, the claims at issue were directed at “synchronizing data between a first system and a second system.” *Id.* at 1361. The defendant Dropbox moved for summary judgment of noninfringement because the claims “all required hardware, but [defendant’s] accused software could not meet that requirement.” *Id.* at 1364. The court granted the motion because “all asserted claims . . . required hardware and [plaintiff] did not accuse any Dropbox hardware of infringing.” *Id.* at 1365. On appeal, the patentee argued that “the district court erred in concluding that the asserted claims require hardware” because “the asserted claims . . . recite hardware not as a claim limitation, but merely as . . . ‘the environment in which software operates.’” *Id.* at 1368. The Federal Circuit rejected this argument and held that “[b]ecause Dropbox does not provide its customers with any hardware in conjunction with its accused software, Dropbox does not make, sell, or offer for sale the complete invention.” *Id.* at 1368.

Dr. Rubin’s infringement theory requires a combination of various Microsoft software *and additional hardware*. See Ex. 3, Rubin Dep. 52:16-20 (“Q. Okay. Do you agree that in Claim 1 of the ’954 patent, an integrated device includes hardware? A. I think an integrated device would include hardware. That would be the environment in which this claim would operate.”). Dr. Rubin identified Microsoft’s software (Windows 10, Windows 11, Office 365, and Microsoft 365) as being involved in performing the claimed method. However, *Dr Rubin does not identify any Microsoft provided hardware for his infringement theory*. Ex. 3, Rubin Dep. 167:5-9 (“Q. Did you include Samsung laptops in your analysis? A. I did not specifically call out Samsung. I was focused on the Windows Hello protocol, and I *don’t have any specific mention of any brands of hardware*.”). Therefore, Microsoft does not *directly* infringe the method claims under Dr. Rubin’s theory.⁴

Similarly, Dr. Cole also only alleged damages based on software. Ex. 4, Cole Dep. 157:13-15 (“Q. When you say “100 percent for Windows,” on your apportionment, is that including hardware? A. That’s the Windows 11 operating system.”); 62:2-7 (“Q. What does the 100 percent at the top encompass? A. That’s the Microsoft 365 product. Q. Does this include hardware? A. I believe this includes the software for Microsoft 365.”). Likewise, Dr. Vanderhart calculates damages based purely on software (*e.g.*, Windows 10, Windows 11, Office 365, Microsoft 365), not hardware. Ex. 5, Vanderhart Op. Rep. ¶¶ 55-64.

3. Proxense Does Not Argue Any Divided Infringement Theory

Finally, Proxense has waived any argument that Microsoft is liable under some divided infringement theory. Regardless, Proxense has not provided any argument that Microsoft directs

⁴ If anything, Proxense would need to perform an indirect infringement analysis which Proxense does not allege. Ex. 3, Rubin Dep. 181:3-5 (“Q. Do you do an indirect infringement analysis anywhere in your report? A. No.”).

and controls the actions of the users. *See ESW Holdings v. Roku*, 6-19-CV-00044-ADA, 2021 WL 1069047, at *4 (W.D. Tex. March 18, 2021) (Albright, J.) (“Roku, in its Reply, contends that mere instruction is not sufficient to prove direction and control of a third-party for the purposes of divided infringement. . . . The Court finds Roku's arguments convincing.”). Nor has Proxense argued that Microsoft “conditions participation in an activity or receipt of a benefit upon performance of” or establishes the manner or timing of that performance. *See Info. Images, LLC v. PGA TOUR, Inc.*, 686 F. Supp. 3d 549, 563 (W.D. Tex. 2023), appeal dismissed, No. 2023-2362, 2023 WL 6784362 (Fed. Cir. Oct. 13, 2023) (granting summary judgment of no direct infringement because both the manner and timing of the claimed step was entirely up to the users and is not dictated by defendant.) (Albright, J.). Furthermore, it is the users themselves that must register their device and set up their device to log in with biometrics. The user must then log in with biometrics with an account that is connected to a Microsoft server while on a wireless network.

For the above reasons, the end-user, not Microsoft, is the accused infringer, so Microsoft is entitled to summary judgment of no direct infringement.

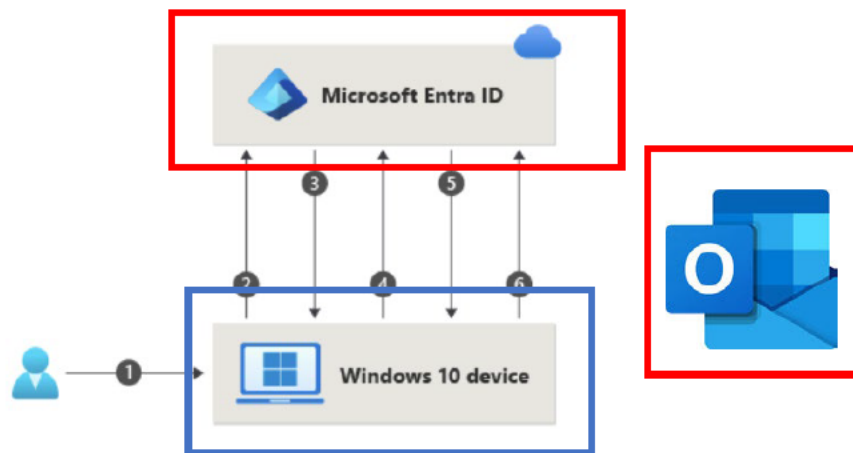
V. MOTION #2: SUMMARY JUDGMENT THAT THE ACCUSED PRODUCTS DO NOT INFRINGE BECAUSE THEY LACK A “THIRD PARTY THAT OPERATES A TRUSTED AUTHORITY”

The remaining independent claim requires a “third party that operates a trusted authority.” Ex. 1, ’954 patent at claim 1. Dr. Rubin’s theory does not satisfy this claim limitation because Dr. Rubin accuses Microsoft of both selling the accused “application[s]” and as being the “third

party.”⁵ Accordingly, there is no “third party that operates a trusted authority” in Dr. Rubin’s infringement theory.

A. There Is No Genuine Dispute of Material Fact

Dr. Rubin explains that “[t]he Accused Products comprise . . . *Microsoft*’s use of passwordless authentication, specifically with biometrics, within Windows Hello and Windows Hello for Business, which are part of Windows 11 and Windows 10 and used for authentication (logging into) *Microsoft*’s subscription services (e.g., *Microsoft* 365 or Office 365).” Ex. 2, Rubin Op. Rep. ¶ 26. As described above, Dr. Rubin’s theory relates to user that log into their device in a way that authenticates with “*Microsoft* Entra ID” (as shown in the diagram below) and then accesses applications. *Id.*, ¶¶ 206-207 (emphasis added) (using image from <https://learn.microsoft.com>). Dr. Rubin alleges that “[a]ll authentication utilizing a *Microsoft* Account to sign in to a Windows 10 / 11 device or *Microsoft* service or product, such as Microsoft 365, to such services is handled by Entra ID.” *Id.*, ¶ 43 (emphasis added).



⁵ This is a separate dispute from Motion #2 that is directed at who is responsible for the accused actions. Indisputably, Dr. Rubin's theory seeks dismissal because the user, not Microsoft, performed the claimed method and fails to show how any party infringes for the additional reason that the Windows software is not sending any data to a "third party." Instead, the user's device is authenticating with Microsoft to access Microsoft applications.

Dr. Rubin’s alleges that the **Microsoft** Entra ID Server is third-party that is separate from the **user’s** Windows device and from the **Microsoft** Account and **Microsoft** 365 application the user is trying to log into. Ex. 2, Rubin Op. Rep. ¶ 334; *id.*, ¶ 333 (“[t]he parties to the transaction are the end-user, . . . and the application being accessed (e.g., the user’s profile, the Windows 10 / 11 device, the user’s **Microsoft** Account, or a **Microsoft** product or subscription).”); Ex. 3, Rubin Dep. 145:24–146:6 (explaining that Microsoft 365 and Office 365 are applications in his infringement theory). Dr. Rubin provides an example of Microsoft 365 application as Outlook. Ex. 2, Rubin Op. Rep. ¶ 244.

However, Dr. Rubin only makes conclusory statements that “**Microsoft** Entra ID is a third party to this transaction.” Ex. 2, Rubin Op. Rep. ¶ 333. For example, Dr. Rubin has not identified any separate “parties” in his infringement theory besides the user and Microsoft (who he alleges makes the Microsoft applications and operates Microsoft Entra ID). Instead, it is clear that there are only two parties to any transaction (1) the end-user (via their Windows computer) and (2) Microsoft (which makes the accused applications and Microsoft Entra ID).

Of course, Microsoft offers an identity service through Microsoft Entra ID for commercial users to access to **Microsoft** applications. *See, e.g.*, Ex. 6, Woodman Dep. 39:17-22 [REDACTED]

[REDACTED]

[REDACTED]

38:9-14 [REDACTED]

[REDACTED]

[REDACTED] There is also no dispute that Dr. Rubin accuses Microsoft of being the “party” behind both the “application” and Microsoft Entra ID as Proxense is requesting damages for Windows and Microsoft 365 (which is only the application in his theory).

Ex. 5, Vanderhart Op. Rep. ¶ 141. Therefore, Microsoft is entitled to judgment as a matter of law that it does not infringe, as Microsoft can not be a “third party” as to itself.

B. Microsoft is Entitled to Summary Judgment: Microsoft Cannot be a “Third Party” to Itself.

Dr. Rubin’s argument is that the “third party” limitation is satisfied because “*Microsoft*’s identity provider server, the *Microsoft* Entra ID Server, is third-party that is *separate from* the user’s Windows device and from the *Microsoft* Account and *Microsoft* 365 application they are trying to log into.” Ex. 2, Rubin Op. Rep. ¶ 334 (emphasis added). Dr. Rubin cannot implicitly construe “third party” to ignore the term’s plain and ordinary meaning to be satisfied by any separate server.

'954 patent claim language	Dr. Rubin’s Infringement Theory
wirelessly sending . . . for authentication to a third party that operates a trusted authority	wirelessly sending . . . for authentication to a ~~third party that operates a trusted authority~~ <i>[separate server]</i>

This broad and conclusory interpretation of “third party” conflicts with the intrinsic evidence and Proxense’s previous statements about this claim limitation to the USPTO. Furthermore, Dr. Rubin’s implicit construction also conflicts with his other infringement opinions (where he explicitly excluded from his theory accusing “third-party applications” to accuse Microsoft applications) and the basis of all of his validity opinions (where Dr. Rubin argued that a “third-party trusted authority . . . would have to be *an entity other than the principal parties* to the transaction”). For these reasons, Microsoft is entitled to judgment as a matter of law.

1. The Intrinsic Evidence Does Not Support the Interpretation of “Third Party” as a Separate Server or Software System Still Belonging to the Same Company

None of the expansive intrinsic evidence of the ’954 patent supports implicitly construing “third party” to encompass a merely separate server controlled by the same party.

a. The Specification of the '954 Patent Does Not Support Dr. Rubin's Implicit Construction

First, the '954 patent specification explicitly explains the benefit of a “third party” to the alleged invention. The alleged invention allows “the integrated device [to] be authenticated for an application that is open to the public (i.e., in an open loop system).” Ex. 1, '954 patent at 3:7-9. The '954 patent explains that “[i]n an open system, where unknown users can attempt authentication (e.g., in a public grocery store), trusted key authority [] provides verification that a key presenting a certain code is legitimate.” Ex. 1, '954 patent at 6:48-51. “By contrast, in a closed system, only known users are legitimate (e.g., owners of a home), the trusted key authority [] can be maintained locally and serves to verify that the key belongs to one of the limited number of users that can use the system.” Ex. 1, '954 patent at 6:51-55.

Dr. Rubin admits that the '954 patent (directly related to the '730 patent) is directed at separating applications from the authentication system. Ex. 7, Rubin Rbtl. Rep. ¶ 399 (arguing that the technical improvement of the '730 patent family is that in the prior art “[w]hen *applications must authenticate* users or other applications for access to password-protected resources, the user and *each third-party application* also has to save the user’s passwords (or other knowledge factor) for that resource. This is insecure because it increases the risk of data breaches exposing the user’s credentials.”) (emphasis added)).

Despite this admitted purpose of the invention, Dr. Rubin accuses **Microsoft** Entra ID as the “third party that operates a trusted authority” while also explicitly limits his infringement theory to “authentication (logging into) **Microsoft**’s subscription services (e.g., Microsoft 365 or Office 365).” Ex. 2, Rubin Op. Rep. ¶ 1; *id.*, ¶ 165 (“the Microsoft user wirelessly sends data to Microsoft Entra ID (Microsoft’s identity provider (IdP) server).”). This is not consistent with the plain and ordinary meaning of the term or purpose of the invention. Therefore, Microsoft Entra

ID is not a “third party,” and “Microsoft is simply keeping track of its own users.” Ex. 8, Schonfeld Rbtl. Rep. ¶ 388; Ex. 9, Dispensa Dep. 20:23-25 (“[REDACTED]”).

b. The '954 Patent Provisional Applications Do Not Support a Broad Reading of Third Party

The '954 patent claims priority to two provisional applications which confirm an interpretation of “third party” consistent with its plain and ordinary meaning to require a different party, not merely a separate server as Dr. Rubin alleges.⁶ In fact, the provisional applications entire focus is on solving issues with third parties’ involvement with biometric data.

The '538 provisional explains the difference between closed-loop and open-loop systems. Ex. 10, at 2. However, the '538 provisional also explains that trying to create an open-loop for biometric authentication “pose[s] far more, and complex, problems/issues.” *Id.* The '538 provisional describes problems with existing “[b]iometric ID security products” such as “inconveniences and privacy-related problems.” *Id.* at 2. Importantly, the '538 provisional explains that a problem at the time was that “[m]ost individuals are simply not comfortable giving their bio data (fingerprints, etc.) to *third parties*.” *Id.* at 3 (emphasis added).

This problem is even worse with existing open-loop models because “to prepare individuals to utilize the technologies, they must have each ‘enroll’ - proving their identity (by showing a driver's license, or similar) and providing a sample of their bio data for storage within the entity’s bio database.” *Id.* at 2. In other words, “[f]or every new entity, the enrollment process must be repeated, representing a considerable hassle to both parties.” *Id.* (emphasis in original). The '538 provisional continues that “much more importantly, it places a significant burden on

⁶ The provisional application (U.S. Provisional Application No. 60/652,765) is substantially similar so only the '538 provisional application is cited below.

entities to securely and accurately manage the process (and acquired data), and opens individuals up to ever-increasing levels of risk.” *Id.* at 3 (“Every entity wishing to utilize such technology must . . . build and maintain its own bio database, properly train personal on the enrollment process, and install critically-important safeguards on the bio data being acquired.”). Therefore, for prior open-loop models with biometric authentication, “every time a user enrolls somewhere, they have released their most private ‘ID’ to one more **third-party**’s confidence.” *Id.* at 3 (emphasis added).

The ’538 provisional describes that with its approach “no actual bio data ever leaves a Bio Key in any way, shape, or manner.” Ex. 10, ’538 provisional at 4 (emphasis in original). The ’538 provisional summarizes that “the PDK Bio Key technology solves significant problems inherent to currently-available biometric technologies” and because “[i]t requires only a single ‘enrollment’ process, it limits the locations at which an individual’s bio data is stored to only one - the owner’s personal Bio Key, and it eliminates the need to provide such data to any **third-party**... ever.” *Id.* at 5 (emphasis in original).

While the ’538 provisional distinguishes and allegedly solved the problem with giving data to third parties, it also taught how to use a “third party” to its advantage. Specifically, the provisional explains how the Bio Key can be validated “by a third party.” *Id.* at 4. The ’538 provisional explains the use of a third party “PDK Central Registry (PCR) - a centralized database controlled by a universally accepted/authorized, unrelated, **third-party** entity” which could “signify[] the Key and owner’s authenticity have been verified.” *Id.* at 9 (emphasis added).

Proxense agrees with this interpretation of the ’538 provisional and the ’954 patent claims’ use of a “third party” trusted authority. Specifically, Proxense has previously argued to this court that the “third party” solves the above identified problems with the open-loop model because “**applications** within an open-loop system are **relieved of the burden of managing authentication**,

and instead have the simpler tasks of sending a code to a third-party trusted authority for authentication and awaiting receipt of an access message.” *Proxense, LLC v. Google LLC*, 6:23-cv-00320-ADA, (W.D. Tex Nov. 26, 2024), Dkt. 120 at 27 (Ex. 11). Therefore, Dr. Rubin cannot now argue that Microsoft is party behind both the “application” and the “third party” which is in direct conflict with the plain and ordinary meaning of the term.

c. The Prosecution History Does Not Support Dr. Rubin’s New Broad Construction

During the prosecution history of the ’730 patent (parent of the ’954 patent), Proxense amended the claims to overcome prior art by adding that the code for authentication was sent “to a third-party” trusted authority. Ex. 12, 2010-02-25 Claim Amendments at 2-5. In the response, Proxense explained that “Amended claim 1 recites a method for verifying a user during authentication where biometric scan data is compared to biometric data and where a code is sent to a **third-party** trusted authority to obtain an **access message** to allow user access.” Ex. 12, 2010-02-25 Response to Rejection at 7 (emphasis in original). According to Proxense, in the prior art, “the communications are limited to data transmissions between the fob 14 and the receiver 15 to obtain access to the door 10.” *Id.* Therefore, “[i]f someone wanted to tamper with the fob 14 to obtain access to the door 10, there is no safety cheek.” *Id.* Proxense then explained that “Claim 1, on the other hand, requires a second level of authentication.” *Id.* at 8. “The authentication process is not completed until a code associated with the integrated device is transmitted to a third party and the third party transmits back an access message.” *Id.*

Proxense then distinguished over the prior art where “the user must prove to the same institution that authenticates the fingerprint information that the user is who he purports to be” because in that situation there are only “two parties: the user and the institution. There is no third-

party authority in this passage.” *Id.* at 8 (emphasis in original); *id.* at 9 (“there is no third-party trusted authority to provide an additional layer of authentication.”).

Like in the prior art over which Proxense distinguished, Microsoft is not authenticating with a third party under the term’s plain and ordinary meaning. Dr. Rubin’s new implicit construction was explicitly disavowed in the prosecution history and should be rejected.

d. Proxense’s Statements Made During the IPRs Contradict Dr. Rubin’s Implicit Construction

In related IPR proceedings, Proxense successfully convinced the Board to adopt a construction of “third party” requiring a different “institution or entity.” *See* Ex. 13, IPR2021-01444 (’730 patent) Decision Denying Institution at 14 (“Patent Owner contends that the parties ‘agree that a “third-party trusted authority” is an institution or entity that is outside of the multi-party system (user and application or vendor) that is being authenticated.’ . . . We agree with Patent Owner.”). The Board elaborated that “[t]he plain meaning of ‘third-party trusted authority’ suggests an entity or party separate from the principal parties to a transaction.” *Id.* (citing THE AMERICAN HERITAGE COLLEGE DICTIONARY 1433 (4th ed. 2004) (“‘third party n. . . . 2. One other than the principals involved in a transaction.’”)). This conflicts with Dr. Rubin’s implicit construction where he does not identify any separate “institution or entity” in his infringement theory.

Proxense also argued that the prior art did not satisfy the “third-party trusted authority” limitation because it was using a “cloud” system and the Board *denied institution on this basis*. *Id.* at 26 (“Patent Owner responds that ‘[Prior art’s Data Processing Center] is part of the system providing access to a user’s registered financial accounts, i.e., a cloud based digital wallet—not a *third party* trusted authority.’”); *Id.* at 27 (“Petitioner does not show persuasively that either Scott or Lapsley teaches a ‘third-party trusted authority,’ as recited in claim 1”). In support of its

decision, the Board agreed with this interpretation and said that this was a similar situation to what applicant distinguished during prosecution. *Id.*; *see supra* Section VI.B.1.c.

Proxense's positions in IPRs directly contradict with Dr. Rubin's infringement theory that Microsoft Entra ID is a third party *because* it is "cloud component." Ex. 2, Rubin Op. Rep. ¶ 206

[REDACTED]

[REDACTED]

[REDACTED] that is separate, and independent from the user's Windows device. Therefore, Microsoft's identity provider server serves as a third party to the user's Windows device.").⁷ While Dr. Rubin's uses the terms "separate" and "independent," his arguments rewrite the claimed "third party" as "third component." *See* Ex. 2, Rubin Op. Rep. ¶ 43 [REDACTED]

[REDACTED]). Proxense cannot "argue[] one way in order to maintain [the '954 patent's] patentability and in a different way against [Microsoft]." *Aylus Networks, Inc. v. Apple Inc.*, 856 F.3d 1353, 1360 (Fed. Cir. 2017); *CUPP Computing AS v. Trend Micro Inc.*, 53 F.4th 1376, 1383 (Fed. Cir. 2022) ("a disclaimer in an IPR proceeding is binding in later proceedings, whether before the PTO or in court."). Therefore, Microsoft is entitled to judgment of noninfringement as a matter of law.

Furthermore, this is not an isolated comment to the Board. Proxense highlights how often it uses this argument as a reason to distinguish prior art in Microsoft and Apple's currently pending IPRs for the '954 patent itself. Ex. 14, IPR2024-00846 POPR at 7-8 ("The USPTO has construed the term 'third-party trusted authority' on six separate occasions. *See Samsung Electronics*

⁷ Dr. Rubin does not provide any doctrine of equivalents analysis for this claim limitation. Ex. 3, Rubin Depo. at 180:23-181:2.

America, Inc. v. Proxense, LLC, IPR2021-01444, Paper 11 at 11-15 (PTAB Feb. 28, 2022); *Samsung Electronics America, Inc. v. Proxense, LLC*, IPR2021-01447, Paper 12 at 10-14 (PTAB Feb. 28, 2022); *Samsung Electronics America, Inc. v. Proxense, LLC*, IPR2021-01448, Paper 12 at 8-11 (PTAB Feb. 28, 2022); *Google, LLC v. Proxense, LLC*, IPR2023-00232, Paper 10 (PTAB Jul. 24, 2024); *Google, LLC v. Proxense, LLC*, IPR2024-00233, Paper 10 (PTAB Jul. 24, 2024); and *Google, LLC v. Proxense, LLC*, IPR2024-00234, Paper 10 (PTAB Jul. 24, 2024). In each instance, the term was construed consistent with its plain and ordinary meaning to mean ‘a trusted authority that is an entity separate from the parties to a transaction.’”).

Dr. Rubin does not acknowledge this repeatedly used construction of the “plain and ordinary meaning” or distinguish the prior art at issue in these decisions. Dr. Rubin even incorrectly alleges that it is “not a proper analysis of the patent or their claims” to use the “the PTAB’s institution decision” with respect to “Third party trusted authority” because it was not construed in those USPTO actions. Ex. 7, Rubin Rbtl. Rep. ¶ 243; *but see* Ex. 15, IPR2024-00846 Patent Owner Response at 2 (“The Board has maintained its **construction** of ‘third-party trusted authority’ as ‘a trusted authority that is an entity separate from the parties to a transaction.’ . . . Patent Owner does not dispute this construction, nor has Patent Owner disputed this construction.”). Yet in other parts of his report, Dr. Rubin also explicitly relies on the Board’s holding for “third party.” Ex. 7, Rubin Rbtl. Rep. ¶ 395 (“It is my understanding that the PTAB found that the Scott reference fails to disclose a “third-party trusted authority” as claimed in the ’730 Patent family.”).

For these reasons, Dr. Rubin’s implicit construction for his infringement opinion that a separate server is a “third party” should be rejected as a matter of law.

2. Dr. Rubin’s Argument About a Third Party Being Merely Separate Conflicts with His Other Opinions on Infringement and Validity

Finally, Dr. Rubin’s broader interpretation of “third party” as merely a “separate” component conflicts with his usage of “third party” throughout the rest of his reports and testimony. For example, Dr. Rubin explains that Windows Hello enables “secure access to Windows devices, Microsoft 365 services, and *third-party* applications that support modern authentication protocols like FIDO2 and WebAuthn.” Ex. 2, Rubin Op. Rep. ¶ 96. However, Dr. Rubin only accuses the “use of passwordless authentication with biometrics in Windows Hello to access *Windows* 10 /11, *Microsoft* Accounts, *Office* 365, and *Microsoft* 365 applications and subscriptions.” Ex. 2, Rubin Op. Rep. ¶ 321. Therefore, to implicate Microsoft’s operating system and its applications, Dr. Rubin has to exclude what he described as the “third-party applications” from his infringement theory.

In Dr. Rubin’s validity opinion, Dr. Rubin is unequivocal that a third party must be a separate “entity.” Ex. 7, Rubin Rbtl. Rep. ¶ 145 (“Accordingly, for there to be third-party trusted authority, it would have to be an entity other than the principal parties to the transaction – i.e., the user and the application being accessed.”); Ex. 3, Rubin Dep. 122:10-13 (“when an entity is a party to the transaction and actively interacting with the transaction and is not an external third party, then it can’t satisfy the external third party.”). However, Dr. Rubin never describes “Microsoft Entra ID” as an “entity” separate from Microsoft. Nor can he.

For all the reasons above, Microsoft is entitled to judgment as a matter of law that it does not infringe the claims of the ’954 patent.

VI. MOTION #3: SUMMARY JUDGMENT THAT THE ACCUSED PRODUCTS DO NOT INFRINGE BECAUSE THEY LACK “PERSISTENTLY STORING . . . IN A TAMPER PROOF FORMAT WRITTEN TO A STORAGE ELEMENT ON THE INTEGRATED DEVICE THAT IS NOT CAPABLE OF BEING SUBSEQUENTLY ALTERED”

The remaining claims all require “persistently storing biometric data of a user . . . in a tamper proof format written to a storage element on the integrated device that is *not capable of being subsequently altered*.” Dr. Rubin’s theory does not satisfy the final “not capable of being subsequently altered” requirement.

Specifically, Dr. Rubin accuses various data of satisfying the “not capable of being subsequently altered” limitation merely because that data is “encrypted,” this data cannot be “*meaningfully* alter[ed].” Ex. 2, Rubin Op. Rep. ¶¶ 110, 114. Dr. Schonfeld explains that, at a minimum, the identified data can be deleted, and he confirmed this by reviewing source code and via testing. *See, e.g.*, Ex. 8, Schonfeld Rbtl. Rep. ¶¶ 273-275. Dr. Rubin has not argued anywhere that the identified data cannot be deleted. Dr. Rubin only argues that “deleting” is not a type of “altering” merely because it does not “change something so that it can be *meaningfully used* in a way it wasn’t supposed to be.” Ex. 3, Rubin Dep. 53:10-14. Dr. Rubin’s late implicit claim construction argument to inject the qualifier “meaningfully” is untimely and should be waived.

'954 patent claim language	Dr. Rubin’s Infringement Theory
persistently storing biometric data . . . in a tamper proof format written to a storage element on the integrated device that is not capable of being subsequently altered	persistently storing biometric data . . . in a tamper proof format written to a storage element on the integrated device that is not capable of being subsequently <i>meaningfully</i> altered

Therefore, Microsoft is entitled to judgment as a matter of law of noninfringement because Dr. Rubin fails to identify data “not capable of being subsequently altered” under its plain and ordinary meaning. In fact, Dr. Rubin’s attempt to justify why “encrypted” data satisfies the claim limitation effectively admits that the accused data can be “altered.” Namely, Dr. Rubin’s argument is that

If someone were to attempt to *alter* data while encrypted, the *alternations* would cause the data to be decrypted incorrectly during authentication. As [sic] authentication would fail. Furthermore, the encrypted data would be gibberish and in no way resemble the underlying biometric template. Consequently, it would be impossible to determine how to

meaningfully alter the biometric data to permit another to log in as the user. The very act of encrypting the data, therefore, writes the biometric in a tamper proof format to a storage element on the Windows 10 / 11 integrated device that is unable to be subsequently altered.

Ex. 2, Rubin Op. Rep. ¶ 110. Dr. Rubin repeats this same argument throughout his report without explaining how the data could not be “altered” generally. *See* Ex. 2, Rubin Op. Rep. ¶ 114 (“The encryption makes it impossible to meaningfully alter the data, and if the data were altered, it would decrypt incorrectly and not permit authentication of the user.”).

Dr. Rubin’s new implicit claim construction also conflicts with the intrinsic evidence and should be rejected on the merits. For example, the ’954 patent distinguishes between the concepts of an element that can “be written to once but cannot be subsequently altered” and data merely stored “in an encrypted form.” Ex. 1, ’954 patent at 5:22-35 (“In one embodiment, at least some of persistent storage 226 is a memory element that can be *written to once but cannot subsequently be altered*. . . . Furthermore, data can be *stored in an encrypted form*.”).

Proxense even explicitly disavowed Dr. Rubin’s encryption theory to overcome prior art during the prosecution of the ’954 patent. Specifically, Proxense amended the claims to add “not capable of being subsequently altered” to overcome U.S. Patent No. 6,041,410 (“Hsu”), which related to use of biometric information for data protection, such as storing a hash of the fingerprint or encrypting the fingerprint. Ex. 16 at 13 (’954 patent file history April 2, 2014 Amendment). However, the prior art also allowed for a switch to be flipped at any point in time to allow for enrollment of additional or other biometric information. *Id.* at 12. Accordingly, Proxense distinguished Hsu by pointing out that even if Hsu is “*encrypting* the fingerprint,” the “fingerprint *may be repeatedly altered, e.g., by overwriting it* with a new fingerprint during re-enrollment.” *Id.* at 13. The examiner accepted this argument and said that “Hsu at most discloses choosing not to alter under normal circumstances and Applicant teaches ‘not capable of being subsequently

altered.” *Id.* at 13. Therefore, Dr. Rubin cannot now allege that “not capable of being subsequently altered” can be satisfied with encryption alone when Proxense explicitly distinguished the concept to obtain the ’954 patent.

The intrinsic evidence also confirms that the invention was directed at storing in a format where the data could not be deleted. This Court already confirmed that “altering” prevents the removal (or deleting) of data based on the same specification in the ’730 patent. Specifically, the Court explained that in the embodiment where the data “cannot subsequently be altered,” the “tamper-proofing prevents altering an instance of stored data by adding to it or modifying it, such that features cannot be added to or **removed** from saved biometric data.” *Proxense LLC v. Samsung Co, Ltd.*, No. 6:21-cv-00210-ADA (W.D. Tex. Dec. 28, 2022), Dkt. No. 149 at 14 (Ex. 32) (citing ’730 patent at 4:31–33, 4:38–41).

Additionally, the ’538 provisional repeatedly describes how data cannot be “deleted” in the described system:

In order to utilize a Bio Key’s biometric capabilities, the intended user/owner must first perform an Owner Initialization Procedure (OIP). An OIP, which can only be run one time, consists of reading, verifying and permanently storing a number of bio scans (e.g. fingerprints) in the Key’s internal bio database. While the OIP may allow for corrections (e.g. re-reads) during the process, once completed, any data acquired is permanently stored . . . unable to ever be modified, **deleted**, added-to, viewed, or (externally) read. If an OIP is incorrectly completed, the Key must be discarded.

Ex. 10, ’538 provisional at 6; *id.* at 8 (“If they chose to complete the process, data from each unique scan (i.e. if the same print was scanned multiple times, only one instance is recognized) is permanently stored in the Key’s internal bio database, where it can never be added-to, **deleted**, modified, viewed or (externally) read.” (emphasis added)).

For all of the above reasons, Microsoft is entitled to judgment as a matter of law of noninfringement based on this limitation as well.

VII. MOTION #4: SUMMARY JUDGMENT THAT THE CLAIMS ARE INVALID UNDER § 101

A. *Alice* Step One: The '954 Patent Claims Are Directed to an Abstract Idea

The '954 patent is directed to the abstract idea of authenticating a person based on biological characteristics and authenticating a physical object they possess with a third party. Proxense's own expert Dr. Rubin offers an apt analogy of "point card issued by a coffee shop" as "[a] good way to think of it." Ex. 7, Rubin Rbtl. Rep. ¶¶ 388-90. For example, the "card itself establishes the identity of a person as a customer of the shop." *Id.* at ¶ 388. Dr. Rubin explains that "[t]he points card is presented to the barista as proof that the customer has been authenticated as a customer of the coffee shop (authentication)." *Id.* ¶ 389.

Adopting Dr. Rubin's analogy, the point card may also have a photograph of the customer's face (biological characteristics) so that the barista may compare it with the person presenting the card. The combination of authenticating both the biological characteristics and verifying that the card is authentic is the abstract idea of the '954 patent. The coffee shop may even store a number in the card and scan it to further verify the authenticity of the card in their systems. A neighborhood small coffee shop may even contract with another company (third party) to run their point card system for them.

Such authentication techniques that have been used long before the '954 patent's priority date, confirming they are directed to patent ineligible abstract ideas under *Alice* Step One. *See Intell. Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1314 (Fed. Cir. 2016) (claiming a "long-prevalent practice" without "improv[ing] the functioning of the computer itself" is an abstract idea). A police officer making a traffic stop first biometrically verifies the identity of the driver by comparing the driver to the photo in his or her driver's license, and also verifies the driver's car by running the license plate against the DMV's record. A TSA agent similarly first verifies the

traveler using his or her driver's license, and then also scan's the traveler's boarding pass to confirm he or she is on the airline's flight manifest. Indeed, the abstract of the '954 patent provides an embodiment of sending data "to an agent for authentication." Ex. 1, '954 patent at Abstract. The '954 patent specification explains that such an "agent can be, for example, a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness." Ex. 1, '954 patent at 7:31-33.

The Federal Circuit has explained that even for "authentication technology," "patent eligibility often turns on whether the claims provide sufficient specificity to constitute an improvement to computer functionality itself." *Universal Secure Registry LLC v. Apple Inc.*, 10 F.4th 1342, 1346 (Fed. Cir. 2021). In *Universal*, the patent claims at issue required "a biometric sensor configured to receive a biometric input provided by the user," if successful, "activat[ing]e [a] electronic ID device," and then "wirelessly transmit[ing] the encrypted authentication information." *Id.* at 1351-52. The Federal Circuit found that these claims are "directed to . . . (1) authenticat[ing] the user based on two factors—biometric information and secret information known to the user—and (2) generat[ing] encrypted authentication information to send to the secure registry through a point-of-sale device." *Id.* at 1352. The "secure registry" then uses the "authentication information" "for authentication . . . and, if authentication is successful, the transaction and access to the user's account is permitted." *Id.* at 1351. The Federal Circuit concluded that the patent claims are "directed to an abstract idea under *Alice* step one" because they merely recite "authenticating a user using conventional tools and generating and transmitting that authentication without 'improv[ing] any underlying technology.'" *Id.* at 1352.

The Federal Circuit's analysis in *Universal* applies equally here, as both the '954 patent claims and the '813 patent claims in *Universal* are directed to authentication techniques with more

than one method. Both patents use biometrics as one authentication technique and sending data (“device ID code” sent to a “third-party trusted authority” in the ’954 patent; “authentication information” sent to a “secure registry” in the ’813 patent) as another authentication technique. The ’954 patent is thus directed to a patent ineligible abstract idea for largely the same reasons that led the Federal Circuit to invalidate the ’813 patent in *Universal*. Namely, here “the asserted claims are directed to a method for verifying the identity of a user to [allow[] the user access to the application], for which computers are merely used in a conventional way, rather than a technological improvement to computer functionality itself.” *See id.* at 1350; Ex. 1, ’954 patent at Claim 1.

Furthermore, the asserted ’954 patent claims do not have “sufficient specificity to constitute an improvement to computer functionality itself” and lack any implementation details and instead merely recite a series of steps to be performed by existing computer technology to implement an abstract idea. *Id.* at 1346; *See Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350, 1356 (Fed. Cir. 2016) (“[T]he essentially result-focused, functional character of claim language has been a frequent feature of claims held ineligible under § 101”). Claim 1 is representative (*see* Section VII.C) and merely shows the combination of these two authentication methods described above (user and device). These concepts permeate all limitations of the independent claims, which require storing the “biometric data” and “device ID code” used for those authentication purposes (“persistently storing . . .” step), authenticating the user via “biometric verification” (“receiving scan data . . .” and “comparing the scan data . . .” steps), and then authenticating the device by sending the “device ID code” to a “third party that operates a trusted authority” for “authentication” and “allowing the user access to the application” (“wirelessly sending” and “receiving . . . an access message” steps). .

Moreover, the specification of the '954 patent confirms that the claimed authentication method merely uses computer technology as a tool rather than improve computer technology itself. The "Background" section of the specification acknowledges that "user authentication techniques . . . designed to prevent access by unauthorized users" were "[c]onventional" even as of the filing of the '954 patent. Ex. 1, '954 patent at 1:26-27. But according to the '954 patent, existing authentication techniques suffered from limitations because "access object[s]" can be "stolen," and coupling them with "credentials (e.g., passwords and PINs)" then required "making the user memorize credentials." *Id.* at 1:31-56. Rather than propose any new authentication technology to address prior technological limitations, however, Proxense merely proposed replacing use of "credentials" from well-known "hybrid authentication techniques" with "conventional" biometrics to avoid requiring the user to "memorize credentials." *Id.* at 1:46-51, 5:11-12. That is an abstract idea.

The fact that the '954 patent claims merely use computer technology as a tool to implement an abstract idea, rather than present any improvement to computer technology, is underscored by the use of "conventional" biometric technology (so no improvement to technology there) and the fact that the claimed second authentication is performed by "third party that operates a trusted authority," which the specification explains is merely a human being (so again, no improvement to any technology). Ex. 1, '954 patent at 5:11-12; 7:30-36; *see also Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350, 1354 (Fed. Cir. 2016) (invalidating patent where "the focus of the claims is not on such an improvement in computers as tools, but on certain independently abstract ideas that use computers as tools"). Indeed, the asserted '954 patent claims lack any implementation details that could be considered an improvement to computer technology, and instead merely recite a series of steps to be performed by existing computer technology to

implement an abstract idea (two factor authentication). *See id.* at 1356 (“[T]he essentially result-focused, functional character of claim language has been a frequent feature of claims held ineligible under § 101”).

In addition, Proxense’s continued emphasis on the claimed “third-party trusted authority” as the central distinguishing feature of the ’954 patent claims over the prior art further reinforces their abstractness. *See* Ex. 7, Rubin Rbtl. Rep. ¶ 144. In *Alice Corp. Ltd. v. CLS Bank International*, 573 U.S. 208, 220 (2014), the Supreme Court held that such “use of a third-party intermediary . . . is also a building block of the modern economy” and thus an abstract idea. That the ’954 patent claims use a similar “third-party” to send an “access message . . . allowing the user access to an application” also does not save the claims, since the claimed “application” can be virtually anything. *See* ’954 Patent at 6:18-34 (“Application 330 can be, for example, a casino machine, a keyless lock, a garage door opener. . .”); *Chamberlain Group, Inc. v. Techtronic Industries Co.*, 935 F.3d 1341, 1345 (Fed. Cir. 2019) (invalidating a patent related to “a garage door” access control system). Even if the claimed “application” were limited to allowing access to computer technology, that would not save the claims, as the focus remains on abstract ideas. *See Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App’x 1014, 1016-1018 (Fed. Cir. 2017) (invalidating under *Alice* claims directed to “control[ling] access to protected computer resources by authenticating identity data, i.e., unique identifying information of computer components”).

B. *Alice* Step Two: The ’954 Patent Claims Lack an Inventive Concept

The ’954 patent claims lack any inventive concept sufficient to confer patent eligibility under *Alice* Step Two. The claims recite nothing beyond generic, conventional, routine computer technology. Ex. 33, Schonfeld Op. Rep. ¶¶ 707-709. For biometric verification, the specification points only to “[c]onventional techniques.” Ex. 1, ’954 patent at 5:11-12. For “persistently storing” in a “in a tamper proof format” and “a storage element . . . that is not capable of being

subsequently altered,” the ’954 patent points only to generic, off-the-shelf read-only-memory (“ROM”) elements. *Id.* at 5:26-29; *see also Chamberlain*, 935 F.3d at 1349 (Fed. Cir. 2019) (no “inventive concept” where claims “could be performed with off-the-shelf technology”). Use of a unique “device ID code” in lieu of a password is also not an inventive concept. *See Prism*, 696 F. App’x at 1017-18 (holding, on a post-trial motion for JMOL, that use of “hardware identifiers” for “provid[ing] secure access over a protected computer resource” was not an inventive concept).

Finally, the “sending,” “receiving,” and “allowing access” steps are equally generic. *See Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 714-15 (Fed. Cir. 2014) (claims requiring “receiving” media and “allowing . . . access to the media” lack inventive concept). Nor does the ordered combination of these steps accomplish anything beyond implementing the abstract idea identified in *Alice* Step One. The only aspect of these claims Proxense consistently argues was missing from the prior art—including across multiple IPRs, reexaminations, and district court cases—is the use of a trusted third party.⁸ But since use of a trusted third party is merely part of the abstract idea, it cannot supply the missing inventive concept. *See BSG Tech LLC v. Buyseasons, Inc.*, 899 F.3d 1281, 1291 (Fed. Cir. 2018) (“[N]arrowing or reformulating an abstract idea does not add ‘significantly more’ to it.”).

Accordingly, there is no genuine dispute of material fact that the asserted ’954 patent claims also fail *Alice* Step Two, rendering summary judgment of invalidity appropriate.

⁸ While Dr. Rubin submitted a validity report on *Alice* Step Two, he stated therein that “I do not believe that Dr. Schonfeld is qualified to discuss whether the claims are patent-eligible.” Ex. 7, Rubin Rbtl. Rep. ¶ 397 fn. 14. If Dr. Schonfeld is unqualified to opine on *Alice* Step Two, then so is Dr. Rubin. Even if considered, Dr. Rubin’s opinions on *Alice* Step Two do not compel a different outcome, as his identification of a “device ID” as an inventive concept is contrary to the Federal Circuit’s decision in *Prism*.

C. Representative Claim Analysis

Claim 1 is “substantially similar and linked to the same abstract idea,” and therefore representative of all the claims in the ’954 patent. *See Mobile Acuity Ltd., v. Blippar Ltd.*, 110 F.4th 1280, 1291 (Fed. Cir. 2024) (quotation omitted). “[B]ecause the other claims’ additional limitations only ‘tack on generic computer components . . . or introduce conventional computer activities,’” and do not depart from the abstract ideas identified above, they are patent ineligible for the same reasons as the representative claims. *Id.* For example, the dependent claims merely “tack on generic computer components . . . or introduce conventional computer activities.” For example, Claim 2 adds a generic “network.” Other claims simply provide example devices (Claim 6) or applications (Claim 7). The remaining claims are directed at biometric techniques conceded by the specification to be conventional. *See* Ex. 1, Claims 3 and 5.

VIII. MOTION #5: THERE ARE NO GENUINE ISSUES OF MATERIAL FACT REGARDING THE LACK OF WILLFUL INFRINGEMENT

A. Factual Background

On May 2, 2023, Proxense filed its original Complaint alleging willful infringement of the ’954 patent. Dkt. 1 ¶¶ 41-45. Proxense’s willfulness allegations hinged entirely on a July 29, 2016 letter from Proxense to Microsoft that listed dozens of patents and patent applications, including the ’954 patent. *Id.*, ¶ 42. Two months later, the parties filed a joint motion to dismiss Proxense’s pre-suit willful infringement claims without prejudice. Dkt. 19.

On April 2, 2025, Proxense sought leave to amend its Complaint to re-plead its willfulness allegations based on “newly produced documents” and the deposition testimony of Michael Perla. Dkt. 85 at 4-5. Yet, even with this evidence, Proxense’s willfulness allegations in its Amended Complaint (Dkt. 93) mirrors the exact language of its willfulness allegations in its original Complaint (Dkt. 1). The Amended Complaint *still* lacks any allegations showing that Microsoft

had any specific knowledge of the '954 patent and/or any infringement thereof. Proxense subsequently served a supplemental response to Microsoft's Interrogatory No. 12 regarding Proxense's basis for its willfulness allegations. Ex. 17 at 5-6 (Proxense's Amd Supp. Resp. to Microsoft's 1st ROGs). Proxense cites several documents, negotiations, and deposition testimony of multiple witnesses (*e.g.*, Michael Perla, John Giobbi, etc.). But again, *none* of this cited evidence has any discussion of any alleged infringement by Microsoft of the '954 patent. *Id.* Microsoft's first awareness of Proxense's allegations of infringement of this patent is—and remains—the filing of Proxense's original Complaint. *See* Ex. 18 at 47 (Microsoft's Sixth Supp. Objs and Resps to Proxense's 1st Set of Rogs).

B. Legal Standard – Willful Infringement

Willful infringement is a fact question requiring a finding of deliberate or intentional infringement. *SRI Int'l, Inc. v. Cisco Sys., Inc.*, 14 F.4th 1323, 1330 (Fed. Cir. 2021), cert. denied, 142 S. Ct. 2732 (2022) (“SRI IV”). As such, summary judgment must be granted when “there is an absence of evidence to support the nonmoving party's case.” *Celotex Corp. v. Catrett*, 477 U.S. 317, 325 (1986); *Novartis Corp. v. Ben Venue Labs., Inc.*, 271 F.3d 1043, 1054 (Fed. Cir. 2001) (affirming district court's grant of summary judgment, finding there were “no facts in the record” to support plaintiff's infringement theory). “Knowledge of the asserted patent and evidence of infringement is [sic] necessary, but not sufficient, for a finding of willfulness.” *Bayer Healthcare LLC v. Baxalta Inc.*, 989 F.3d 964, 988 (Fed. Cir. 2021).

To prove willfulness, Proxense also “must show that [Microsoft] had a specific intent to infringe at the time of the challenged conduct.” *BASF Plant Sci., LP v. Commonwealth Sci. & Indus. Research Org.*, 28 F.4th 1247, 1274 (Fed. Cir. 2022). Specific intent requires, at a minimum, knowledge that an act constitutes infringement, and a disregard of the same. *See Boston*

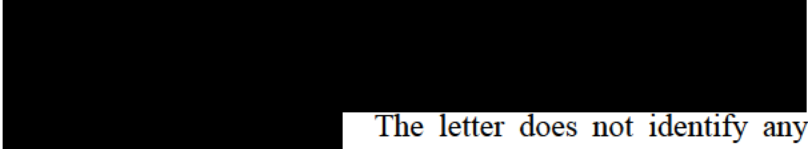
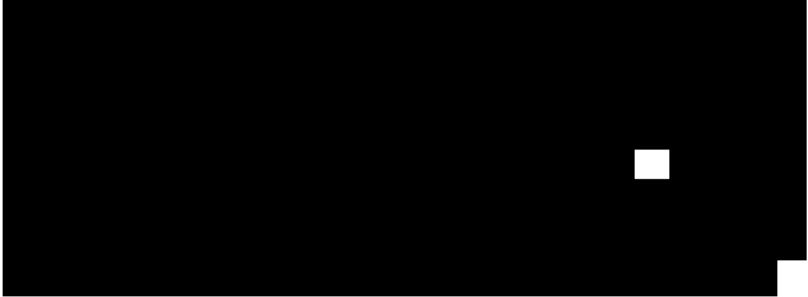
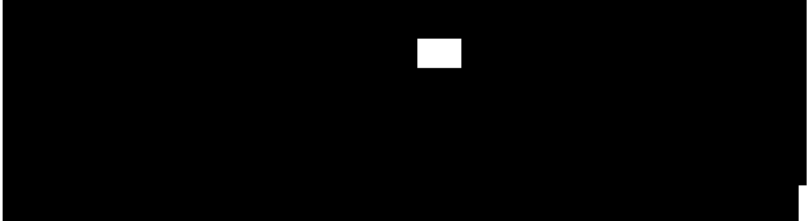
Scientific Corp. v. Nevro Corp., 560 F. Supp. 3d 837, 842 (D. Del. 2021); *Halo Elecs., Inc. v. Pulse Elecs., Inc.*, 579 U.S. 93, 103-04 (2016).

C. Proxense’s Claim for Pre-Suit Willfulness Fails Because It Has Not Shown that Microsoft Had Pre-Suit Knowledge of the ’954 Patent

None of Proxense’s cited evidence establishes that Microsoft had specific knowledge of the ’954 patent, let alone that Microsoft was allegedly infringing the ’954 patent. Microsoft’s general knowledge of Proxense’s patent portfolio and/or Proxense’s technology is insufficient to establish the requisite knowledge for pre-suit willful infringement. *HOYA Corp. v. Alcon Inc.*, 713 F. Supp. 3d 291, 317 (N.D. Tex. 2024) (“Knowledge of a patent portfolio generally is not the same thing as knowledge of a specific patent.”); *see also Bayer Healthcare*, 989 F.3d at 988 (rejecting willfulness argument that the accused infringer learned of the patent from “prior dealings” and holding that the evidence “merely demonstrat[ed infringer’s] knowledge of the [asserted] patent and [infringer’s] direct infringement of the asserted claims” and therefore did not rise to “deliberate or intentional infringement”).

First, Microsoft never received any pre-suit documents or communications from Proxense claiming that Microsoft was infringing the ’954 patent. For example, Proxense’s July 29, 2016, letter to Microsoft includes broad references to “Proxense’s ‘over 30 patents’” and “another 20+ US patent applications pending.” Dkt. 93, Ex. 10. Nothing in this letter calls Microsoft’s attention to the ’954 patent, much less alleges that Microsoft is infringing the ’954 patent.

Second, as shown in the table below, in its supplemental response to Microsoft’s Interrogatory No. 12, Proxense cites dozens of documents regarding the “parties continued negotiations,” but notably, Proxense is silent as to which—if any—of the documents contain specific discussions about the ’954 patent. Ex. 17 at 5-6.

Category	Exemplary Documents ⁹
2008 Communications Between Proxense and Microsoft	 No specific patents were identified and no claim charts were provided. See Ex. 19 ( PROX MSFT 062331)
2010 Communications Between Proxense and Microsoft	 The letter does not identify any patents and does not include any claim charts. See Ex. 20 ( (PROX MSFT 062268))
2016 Communications Between Proxense and Microsoft	 See Exs. 21 and 22 (Email fr  (PROX MSFT 003531 and MSFT PROXE000195263))
2021-2022 Communications Between Proxense and Microsoft	 No claim charts were provided.

⁹ Proxense's Supplemental Response includes over 30+ documents, which can be found in Ex. 2 at 5-6. For purposes of this motion, Microsoft has identified exemplary documents for each of the categories provided in the table above.

¹⁰ Proxense represented that it would not rely on the TruProx product as practicing the Asserted Patent at trial.

	See Ex. 23 (Email fr [REDACTED] [REDACTED] (MSFT_PROXE000462948))
--	--

As an initial matter, the application for the '954 patent was filed on December 12, 2012, and issued on November 11, 2014. Thus, Microsoft could not have had an awareness of the '954 patent during its 2008 and 2010 communications with Proxense because the application for the '954 patent *had not even been filed* with the U.S. Patent and Trademark Office yet. No claim charts were ever exchanged between the parties regarding Microsoft's alleged infringement of the '954 Patent. Ex. 17 at 5-6. Proxense does not cite any presentations that mapped any of Microsoft's products to any exemplary claims of the '954 patent. *Id.* And Proxense does not point to any communications where Proxense affirmatively identifies a Microsoft product that purportedly infringes the '954 patent. *Id.*

The *only* document that Proxense highlights in its Interrogatory response [REDACTED]

[REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]. See Ex. 24 (MSFT_PROXE000462788). [REDACTED]

[REDACTED] *Id.* This is insufficient to establish knowledge of the patent, as no Microsoft witness testified that it ever reviewed that entry or spreadsheet. Even so, *at most*, this document shows mere knowledge of the '954 patent, which is insufficient to establish a claim of willfulness.

Multiple witnesses confirm that Microsoft did *not* have specific knowledge of any alleged infringement of the '954 patent by Microsoft. For example, Proxense identified Mr. Michael Perla, a former Microsoft employee, as a person with knowledge as to pre-suit willfulness. Ex. 17 at 5. Mr. Perla, however, could not have had knowledge regarding the '954 patent during his time at Microsoft because (1) Mr. Perla had left Microsoft in 2012 and (2) as discussed above, the '954

patent was not even issued (and was not even filed with the PTO) yet. Ex. 25, Perla Dep. Tr. at 54:12-22, 55:16-19, 60:7-16. Nonetheless, Mr. Perla further confirmed that Proxense never shared information about its patents and Proxense never stated or claimed that Microsoft infringed Proxense's patents. *Id.* at 59:11-17. To the extent any Proxense confidential information was provided to Mr. Perla, none of that confidential information was ever shared with Microsoft engineers. *Id.* at 58:15-24. Mr. Perla had even specifically instructed Proxense not to share any trade secrets with Microsoft. *Id.* And Proxense's own corporate representative, Mr. John Giobbi, did not remember informing Microsoft of any alleged infringement or any specific patents. *See e.g.*, Ex. 26, Giobbi Tr. at 184:9-14 ("Q. And what exactly did you tell Microsoft about what it was infringing? . . . A. I don't remember, I really don't. I'm sorry."); 186:16-20 ("Q. Okay. And did you identify any specific patents on those calls? A. I don't know. I have no idea. I barely remember the conversations anymore, you know, but I don't know."); 192:18-193:2 ("Q. Okay. And did you walk through the claims with Microsoft in your patents? A. No. I don't know.").

No reasonable jury can find pre-suit willful infringement based on these assertions because Proxense has provided *no* evidence to show that Microsoft knew about the '954 patent, much less knew about any infringement allegations.

D. Proxense's Post-Suit Willfulness Claim Also Fails Because Proxense Has Identified No Evidence of Intent to Infringe

Proxense's post-suit willfulness claim fares no better. Proxense relies *solely* on Microsoft's continued commercial activities as its basis for its post-suit willfulness claims. Dkt. 93 ¶ 45. Without more, there can be no genuine dispute of material fact with respect to post-suit willfulness. *See Gustafson, Inc. v. Intersystems Indus. Prods., Inc.*, 897 F.2d 508, 511 (Fed. Cir. 1990) ("Nor is there a universal rule that to avoid willfulness one must cease manufacture of a product immediately upon learning of a patent, or upon receipt of a patentee's charge of infringement, or

upon the filing of suit.”); *HOYA Corp.*, 713 F. Supp. at 318 (finding that the continued sale of the Accused Product “without more, is insufficient to create a fact question as to willfulness”).

Moreover, during the litigation, Microsoft served non-infringement contentions, served invalidity contentions, and filed an IPR that has been instituted. Ex. 18, 2025-03-11 Microsoft Corporation’s Sixth Supplemental Responses and Objections to Plaintiff Proxense, LLC’s First Set of Interrogatories (NOS. 1-17) at 11-46; Ex. 27, 2025-01-10 Microsoft’s Final Invalidity Contentions; Ex. 28, IPR2024-00846 Decision Granting Institution of Inter Partes Review. In fact, Microsoft’s IPR is not the only one that has been instituted; Apple and Google also filed instituted IPRs. Ex. 29, IPR2024-00233 Decision Granting Institution of Inter Partes Review; *id.*, IPR2024-01334 Decision Granting Institution of Inter Partes Review. And Proxense conceded unpatentability of all claims of the ’730 patent, which is the parent of the ’954 patent and has very similar claims. *See* Ex. 30; *see also* Ex. 31, IPR2024-00233, Document 31 at 8:15-20. Thus, Proxense’s post-suit willfulness claim fails as a matter of law, as Microsoft’s defenses are objectively reasonable and provide a strong basis to show Microsoft did not have a subjective belief it was infringing a valid patent. *WesternGeco*, 837 F.3d at 1363 (“After *Halo*, the objective reasonableness of the accused infringer's positions can still be relevant for the district court to consider when exercising its discretion.”). This is further supported by Microsoft’s strong noninfringement and invalidity positions as described in Motions #1-4.

Indeed, the Federal Circuit has repeatedly found that post-suit willful infringement under the *Halo* standard requires a finding of ***deliberate or intentional*** infringement. *See, e.g., SRI IV*, 14 F.4th at 1330. Where “[t]here is no evidence that shows the defendants subjectively believed [they were] infringing a valid patent,” summary judgment of no post-suit willful infringement is appropriate. *Evolved Wireless, LLC v. Apple Inc.*, C.A. No. 15-542-JFB-SRF, 2019 WL 8128550,

at *4 (D. Del. Feb. 19, 2019) (applying *Halo*). Microsoft’s continued sale of the Accused Products is “standard practice, not egregious, in patent cases . . . where the usual course is that the defendant keeps on selling the accused product or practicing the accused method after the lawsuit is filed.” *See NexStep, Inc. v. Comcast Cable Comm’s, LLC*, No. 19-1031-RGA-SRF, 2021 WL 4077778, at *13 (D. Del. Aug. 20, 2021) (citing *Bioverativ Inc. v. CSL Behring LLC*, C.A. 17-914-RGA, 2020 WL 1332921, at *3 (D. Del. Mar. 23, 2020) (granting summary judgment of no willfulness)). Furthermore, “it seems beyond the pale to expect every patent defendant to ‘cease all allegedly infringing conduct once a complaint is filed’ to force them to avoid enhanced damages for willful infringement.” *Ravgen, Inc. v. Quest Diagnostics Inc.*, No. 2:21-cv-09011-RGK-GJS, 2022 WL 2047613, at *3 (C.D. Cal. Jan. 18, 2022) (dismissing post-suit willfulness claim) (citing *M&C Innovations, LLC v. Igloo Prods. Corp.*, No. 4:17-CV-2372, 2018 WL 4620713, at *5 (S.D. Tex. July 31, 2018)).

Given Proxense’s evidentiary failures, there are no triable factual issues as to willful infringement. However, this Court need not even reach this issue if it grants summary judgment on one of Microsoft’s other four motions.

IX. CONCLUSION

Accordingly, Microsoft respectfully requests the Court to grant the above motions for summary judgment.

Date: June 3, 2025

Respectfully submitted,

/s/ Joseph R. Dorris

Betty Chen
TX Bar No. 24056720
bchen@desmaraisllp.com
DESMARAIS LLP
101 California Street, Suite 3070
San Francisco, CA 94111
Telephone: (415) 573-1900
Facsimile: (415) 573-1901

Jason W. Wolff
CA Bar No. 215819
wolff@fr.com
James Yang
CA Bar No. 323287
jyang@fr.com
FISH & RICHARDSON P.C.
12860 El Camino Real, Suite. 400
San Diego, CA 92130
Telephone: (858) 678-5070
Facsimile: (858) 678-5099

Benjamin C. Elacqua
Texas Bar No. 24055443
elacqua@fr.com
FISH & RICHARDSON P.C.
909 Fannin Street, Suite 2100
Houston, TX 77010
Tel: (713) 654-5300
Fax: (713) 652-0109

Joseph R. Dorris
GA Bar No. 586708
dorris@fr.com
FISH & RICHARDSON P.C.
1180 Peachtree Street, NE, 21st Floor
Atlanta, GA 30127
Telephone: (404) 724-2851
Facsimile: (404) 892-5002

Claire Chang

CA Bar No. 341420
cchang@fr.com
FISH & RICHARDSON P.C.
500 Arguello St, Suite 400
Redwood City, CA 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

Melissa Smith
Texas Bar Number 24001351
melissa@gillamsmithlaw.com
GILLAM & SMITH, LLP
303 South Washington Avenue
Marshall, TX 75670
Tel: (903) 934-8450

**COUNSEL FOR DEFENDANT,
MICROSOFT CORPORATION**

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing document was filed electronically on June 3, 2025. As of this date, all counsel of record have consented to electronic service and are being served with a copy of this document through the Court's CM/ECF system.

/s/ Joseph R. Dorris
Joseph R. Dorris