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

PROXENSE, LLC, Plaintiff, vs. INTEL CORP., Defendant.	Case No. 6:23-cv-283 **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Proxense, LLC ("Proxense" or "Plaintiff") hereby sets forth its Complaint for patent infringement against Defendants Intel Corp. ("Intel" or "Defendant"), and states as follows.

NATURE OF THE CASE

1. This action is for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1, et seq. As further stated herein, Proxense alleges that Intel infringed and continues to infringe one or more claims of patents owned by Proxense. Accordingly, Proxense seeks monetary damages and injunctive relief in this action.

THE PARTIES

2. Plaintiff Proxense, LLC is a Delaware company with its principal place of business at 689 NW Stonepine Drive, Bend, Oregon 97703.

3. On information and belief, Intel is a Delaware corporation with a physical address of 1300 South MoPac Expressway, Austin, Texas 78746, and employs more than 2,000 people in Austin. Intel is registered to do business in the State of Texas and has been registered since 1989

(Texas Taxpayer Number 19416727436 and SOS File Number 0008006206). Intel may be served through its registered agent, CT Corporation System, at 1999 Bryan St., Ste. 900, Dallas, TX 75201.

4. Defendant's past and continuing making, using, selling, offering for sale, and/or importing, and/or inducing its subsidiaries, affiliates, retail partners, and customers in the making, using, selling, offering for sale, and/or importing the accused Wi-Fi compliant devices throughout the United States impermissibly take the significant benefits of Proxense's patented technologies without fair compensation to Proxense.

JURISDICTION AND VENUE

5. This Court has exclusive subject matter jurisdiction over this case pursuant to 28 U.S.C. §§ 1331 and 1338(a) on the grounds that this action arises under the Patent Laws of the United States, 35 U.S.C. § 1 et seq., including, without limitation, 35 U.S.C. §§ 271, 281, 284, and 285.

6. This Court has general and specific personal jurisdiction over Defendant pursuant to due process and/or the Texas Long Arm Statute because, inter alia, (i) Defendants have done and continue to do business in Texas and (ii) Defendants have, directly and through intermediaries, committed and continue to commit acts of patent infringement in the State of Texas, including making, using, offering to sell, and/or selling accused products in Texas, and/or committing a least a portion of any other infringements alleged herein. Notably, Intel developed, made, used, offered to sell, and sold the Intel® Home Wi-Fi Chipset WAV600 Series in or around 2018 and continues to develop, make, use, offer to sell, and sell client-side wireless adapters. Additionally, Intel coordinated with U.S.-based and international router manufacturers in its push for Wi-Fi 6 enabled routers, as it needed such high-speed routers in the market to

work with its wireless adapters in client devices. Accordingly, Defendant has placed, and is continuing to place, infringing products into the stream of commerce via an established distribution channel, with the knowledge and/or understanding that such products are sold in Texas, including in this District. Defendant has derived substantial revenues from its infringing acts occurring within Texas and within this District. Defendant has substantial business in this State and judicial district, including: (A) at least part of their infringing activities alleged herein; and (B) regularly doing or soliciting business, engaging in other persistent conduct, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported, and services provided to Texas residents vicariously through and/or in concert with its alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, and/or consumers.

7. Exercising personal jurisdiction over Defendant in this District would not be unreasonable given Defendant's contacts in this District, the interest in this District of resolving disputes related to products sold herein, and the harm that would occur to Plaintiff.

8. In addition, Defendant has knowingly induced and continues to knowingly induce infringement within this District by coordinating in the development of and/or manufacturing WAV600 Chipsets that are pre-loaded with infringing functionality, incorporated into products sold and offered sale within this District, and that have substantially no non-infringing use. Furthermore, Defendant develops and sells Wi-Fi 6 (Gig+) and Wi-Fi 7 chipsets for laptops and PCs that when operated for their intended purpose with Intel supplied drivers facilitate, direct or encourage the use of infringing functionality with knowledge thereof.

9. With respect to the Asserted Patents, the Accused Products are devices that include, but are not limited to, Defendant's devices that support Wi-Fi 6 and above (e.g., Wi-Fi-7) and/or other devices, as well as their components and processes related to the same.

10. This Court has personal jurisdiction over Intel because Intel is a multinational technology company that has a significant presence in this District through the products and services Intel provides residents of this District.

11. Intel regularly conducts business and has committed acts of patent infringement within this Judicial District that give rise to this action and has established minimum contacts within this forum such that the exercise of jurisdiction over Intel would not offend traditional notions of fair play and substantial justice. Intel has committed and continues to commit acts of infringement in this Judicial District by, among other things, offering to sell, selling, using, importing, and/or making products and services that infringe the asserted patents. Intel has further induced acts of patent infringement by others in this Judicial District and/or has contributed to patent infringement by others in this Judicial District, the State of Texas, and elsewhere in the United States.

12. Intel describes that it is "proud to call Texas home" and has innovated and invested "in Texas for more than 20 years." *See e.g.* https://www.intel.com/content/www/us/en/corporate-responsibility/intel-in-texas.html. "Intel's Austin facility is a research and development center where more than 2,000 employees innovate at the boundaries of technology". *Id.* "The Austin site is focused on supporting innovations in cloud computing, Internet of things, 5G connectivity, memory, and programmable solutions, which are key to driving innovation that makes the world safer, builds healthy and vibrant communities, and increases productivity." *Id.*

13. On information and belief, Intel has authorized retailers in this Judicial District that offer and sell products on its behalf in this District, including products accused of

infringement herein. On information and belief, these include the accused chipsets, wireless adapters and microprocessors.

14. Proxense's causes of action arise directly from Intel's business contacts and other activities in the State of Texas and this District.

15. Intel has derived substantial revenues from its infringing acts within the State of Texas and this District. On information and belief, Intel's revenue was more than $2.1 billion in 2023, with much of that revenue derived from the manufacture of chipsets sold by MaxLinear and sales of its PC and laptop chipsets. On information and belief, and as relevant to this Action, Intel's annual wireless chipset sales exceed one billion dollars.

16. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1400(b). Intel is registered to do business in Texas and, upon information and belief, Intel has transacted business in the Western District of Texas and has a regular and established place of business in this Judicial District and in which Intel conducts its accused infringing acts. Intel maintains a large 61-acre office complex at 1300 South MoPac Expressway, Austin, Texas 78746 with more than 2,000 employees.

17. Among these employees are key witnesses involved in Intel's infringement concerning wireless communications and passwordless related technologies, both of which are relevant to the accused products in this action as described herein. For example:

- Cristina Rodriguez is a Vice President in the Network and Edge Group (NEX), general manager of the group's wireless access network division (WAND) and general manager of the Austin design center at Intel Corporation. Ms. Rodriguez describes on her LinkedIn profile that she "lead[s] Intel's efforts to provide innovative wireless access

solutions." She is located in Austin. See https://www.linkedin.com/in/cristina-rodriguez-8830821/.

- Bryan Boatright is a Vice President in the Silicon Engineering Group and General Manager. Mr. Boatright describes that he "lead[s] Intel's small core development organization responsible for RTL through tapeout including pre- and post-silicon verification." He is located in Austin. See https://linkedin.com/in/bryan-boatright-47b01290/.
- Jagadeesh Nallagatla is Intel's Director of Engineering. He is located in Austin. See https://linkedin.com/in/jagadeesh-nallagatla/.
- Ankit Shah is the Director of Design Engineering at Intel. He is located in Austin. See https://linkedin.com/in/ankitks/.
- Jonathan Devlin is a Director, Wireless Access at Intel Corporation, and he wis located in Austin. See https://www.linkedin.com/in/jonathan-devlin-259a203/.

18. Defendant is a member of the Wi-Fi Alliance, which has its headquarters in Austin, Texas. *See* https://www.wi-fi.org/membership/member-companies; https://www.wi-fi.org/contact-us. "Membership in Wi-Fi Alliance® shows [a] business is engaged in the latest Wi-Fi® technology developments." https://www.wi-fi.org/membership.

PATENTS-IN-SUIT

19. On July 20, 2012, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,219,129 (the "129 Patent") entitled "Dynamic Real-Time Tiered Client Access." A true and correct copy of the 129 Patent is attached hereto as **Exhibit 1**.

20. On June 4, 2013, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,457,672 (the "672 Patent") entitled "Dynamic Real-Time Tiered Client Access." A true and correct copy of the 672 Patent is attached hereto as **Exhibit 2**.

21. On February 16, 2016, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,265,043 (the "043 Patent") entitled "Dynamic Real-Time Tiered Client Access." A true and correct copy of the 043 Patent is attached hereto as **Exhibit 3**.

22. On October 11, 2011, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,036,152 (the "152 Patent") entitled "Integrated Power Management of a Client Device Via System Time Slot Assignment." A true and correct copy of the 152 Patent is attached hereto as **Exhibit 4**.

23. On January 8, 2013, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,352,730 (the "730 Patent") entitled "Biometric Personal Data Key (PDK) Authentication." A true and correct copy of the 730 Patent is attached hereto as **Exhibit 5**.

24. Proxense is the sole and exclusive owner of all right, title, and interest to and in, or is the exclusive licensee with the right to sue for, the 129, 672, 043, 152, and 730 Patents (together, the "Patents-in-Suit"), and holds the exclusive right to take all actions necessary to enforce its rights to the Patents-in-Suit, including the filing of this patent infringement lawsuit. Proxense also has the right to recover all damages for past, present, and future infringement of the Patents-in-Suit and to seek injunctive relief as appropriate under the law.

25. The technologies of the Patents-in-Suit were invented by John Giobbi, David Brown, and Fred Hirt. The 129, 672, and 043 Patents generally cover systems and methods for client devices in a wireless network that share timeslots in a dynamic tiered manner. The 152

Patent generally covers apparatus and methods for network devices that alternate between active and sleep modes based on assignment information.

26. The 730 Patent generally covers systems and methods for an integrated device that persistently stores biometric data for a user in a tamper-resistant format for authentication purposes.

FACTUAL ALLEGATIONS

I. PROXENSE AND ITS INNOVATIVE TECHNOLOGIES

27. Proxense was founded in 2001.[1] From approximately 2004-2012, Proxense developed, *inter alia*, wireless technologies and commercial products, employing over thirty engineers, and investing many millions of dollars in product development and other research and development efforts. Foundational capabilities of Proxense's technologies included managing multiple client access to a wireless network whereupon the clients could efficiently share access in a dynamic, tiered manner. They also included a secure element, biometrics captured and stored thereon, retrieval of biometrics and token passing to a trusted third party, and completion of a mobile payment transaction.

28. Proxense also developed sophisticated, proprietary, proximity-based detection, authentication, and automation technology, built on the concept of wirelessly detecting, authenticating, and communicating with personal digital keys ("PDKs"). Proxense's technology enabled PDKs to run for as long as two years on tiny batteries. "ProxPay" technology also included biometrically-based user and device authentication options, the ability to conduct biometric-verified transactions without sending or exposing the underlying biometric data or

[1] The company was formally incorporated as an LLC in 2001 under the name Margent Development LLC; in 2005, the business was renamed to Proxense LLC.

storing it anywhere except the PDK, and the incorporation of a registration for maintaining or verifying the PDK. Significant financial and engineering resources were deployed to make this possible. The resulting developments became primary differentiators of Proxense's product line, and significant elements on which its business was built.

29. John Giobbi is the founder and CEO of Proxense. He is an experienced product designer and prolific inventor (a named inventor on approximately 200 patents, including some of the asserted patents), with over 35 years of experience as an entrepreneur and product development executive. For example, Mr. Giobbi was a Senior Vice President at WMS Gaming, and managed over 200 staff; in his six-year tenure at that company, its market capitalization soared from approximately $80 million to about $1 billion. Mr. Giobbi was also the founder and President of Prelude Technology Corp. and InPen.

30. The innovative, visionary nature of Proxense's technology was recognized in the media, beginning in mid-2008, when, The Bulletin featured a story on Proxense's mobile payment technology, titled "A pint-sized virtual wallet." Andrew Moore, The Bulletin (May 7, 2008), **Exhibit 11**. The story describes a future that greatly resembles the present-day, including a "wireless wallet" and "fingerprint" verification, including the use of such technology to pay for goods using such wireless methods protected by biometric measures like a fingerprint. In 2009, Trend Hunter ran a similar story titled "Virtual Biometric Wallets," featuring Proxense and Mr. Giobbi. Michael Plishka, Trend Hunter (January 4, 2009), *See* **Exhibit 12**.

31. Another 2009 article, ran in DARKReading, a publication in InformationWeek's IT Network, also featured the company and Mr. Giobbi in an article titled "Startup May Just Digitize Your Wallet." George V. Hulme, DARKReading (February 8, 2009), *See* **Exhibit 13**. The DARKReading article described that Proxense was "in the process of bringing to market a

proximity-based communications device that aims to provide a way to securely share information and conduct payments." Proxense's Personal Digital Keys (PDKs) were described as "carried by users, perhaps even within a cell phone, and can security hold data and manage authentication." Mr. Giobbi explained that "the data within the PDK also can be protected by additional layers of authentication, such as biometric…"

32. It would be years until products utilizing these technologies were launched and became mainstream. Indeed, Wi-Fi 6 released in 2019. Likewise, Apple's TouchID, which involves fingerprint recognition technology, was introduced in 2013. It would take Google until 2019 to enable biometric authentication for Android 10 phones and Google Pay. Accordingly, Proxense's technology was years ahead of the industry.

33. Today, Proxense holds 80 patents on related technology, including digital content distribution, digital rights management, managing wireless access, personal authentication, biometric data management, and mobile payments. Proxense continues to prosecute new patents on its proprietary technologies.

II. INFRINGEMENT ALLEGATIONS AND ACCUSED PRODUCTS

1. Intel Wi-Fi 6, Wi-Fi 6E, and Wi-Fi 7 Wireless Adapters

34. Although Intel is best perhaps known for its microprocessors, a substantial part of Intel's business relates to wireless adapters and chipsets, which are compatible with various wireless networking standards. Wi-Fi is a family of wireless network protocols based on the IEEE 802.11 family of standards, which are commonly used for local area networking of devices and Internet access. Wi-Fi 6 is also known as IEEE 802.11ax. Wi-Fi 7 is also known as IEEE 802.11be.

35. The Wi-Fi Alliance is a non-profit organization that owns the Wi-Fi trademark. Manufacturers may use the trademark to brand products certified for Wi-Fi interoperability. It is based in Austin, Texas. Defendant is a member of the Wi-Fi Alliance.

36. Intel has focused on both router and client-side wireless solutions. For example, the Intel® Home Wi-Fi Chipset WAV600 Series, including the WAV654, (Intel's Accused Gateway Products) are "Wi-Fi 6 chipsets for home Wi-Fi routers, gateways, and intelligent range extenders in cable, xDSL, and consumer retail infrastructure." **Exhibit 14** (MaxLinear WAV600 Product Brief), **Exhibit 15** (Intel WAV600 Product Brief) (listing "applications" as including "Service Provider Gateways" and "Routers, Access Points, Extenders & Repeaters."). On the side end of the spectrum, Intel's wireless adapters and Wi-Fi integrated processors are focused on the client side.

37. In or around 2018 Intel designed the Intel Home Wi-Fi Chipset WAV600 Series to comply with the IEEE 802.11ax standard and support Giga-bit Wi-Fi, which Intel described "is future proofed for Wi-Fi 6 clients, and provides the ability to connect up to 256 clients simultaneously, enabling a high-quality user experience for a growing number of connected devices in the home." **Exhibit 15.** Intel optimized these chipsets for the Intel AnyWAN Silicon on Chips (SoCs) and the Intel Puma 7 Family "to fully offload the wireless traffic with zero CPU utilization." *Id.* The chipset offered support for OFDMA (uplink and download) and Target Wake Time (TWT) as described below, "thereby improving network performance and efficiency." *Id.*

38. Intel coordinated with U.S.-based router manufacturers, such as Netgear and TP Link, to include Intel Home Wi-Fi Chipset WAV600 Series in routers sold in the U.S. Intel also coordinated with international manufacturers, like Edimax and Elecom, in its push for Wi-Fi 6-

enabled routers as it needed such high-speed routers in the market to work with its Intel wireless adapters in client devices. See e.g. https://www.mbreviews.com/netgear-rax40-ax4-review/ (teardown revealing that the Netgear AX3000 uses an Intel WAV654 chip, among other Intel silicon) and https://www.techspot.com/news/81711-tp-link-unveils-archer-ax50-first-wi-fi.html (describing that the TP-Link Archer AX50, the company's first Wi-Fi 6 router, uses an Intel Home Wi-Fi WAV654 Chipset).

39. Intel dubbed the ecosystem, which included routers with its WAV600 Series chips as well as PCs and laptops with its wireless adapters, Intel Wi-Fi 6 (Gig+). After the release of its first Wi-Fi 6 router, TP-Link described that the router would pair perfectly "with new Intel Wi-Fi 6 Gig+ PCs and laptops, allowing numerous bandwith-intensive tasks to run smoothly at the same time." *Id*..

40. In August of 2020, Intel sold its Home Gateway Platform Division, centered around the Intel® Home Wi-Fi Chipset WAV600 Series, to the fabless semiconductor company MaxLinear. See https://www.maxlinear.com/news/press-releases/2020/maxlinear-to-acquire-intel%E2%80%99s-home-gateway-platform (April 6, 2020). On information and belief, MaxLinear, a fabless semiconductor company, would still have to rely on Intel's foundries to produce the acquired Home Wi-Fi Chipset WAV600 Series. Additionally, on information and belief, even after the acqusiution MaxLinear and Intel would continue coordinating to ensure future proofing and high-quality user experiences with Intel Wi-Fi 6 (Gig+) enabled laptops and PCs. See **Exhibit 15** (Intel WAV600 Product Brief) ("[Intel Home Wi-Fi Chipset WAV600 Series] … are also future proofed for PCs with Intel® Wi-Fi 6 (Gig+) for the next generation of Gigabit Wi-Fi that will enable high-quality user experiences."); and **Exhibit 14** (MaxLinear WAV600 Product Brief") ("Routers, access points and gateways based on the Wi-Fi Chipset

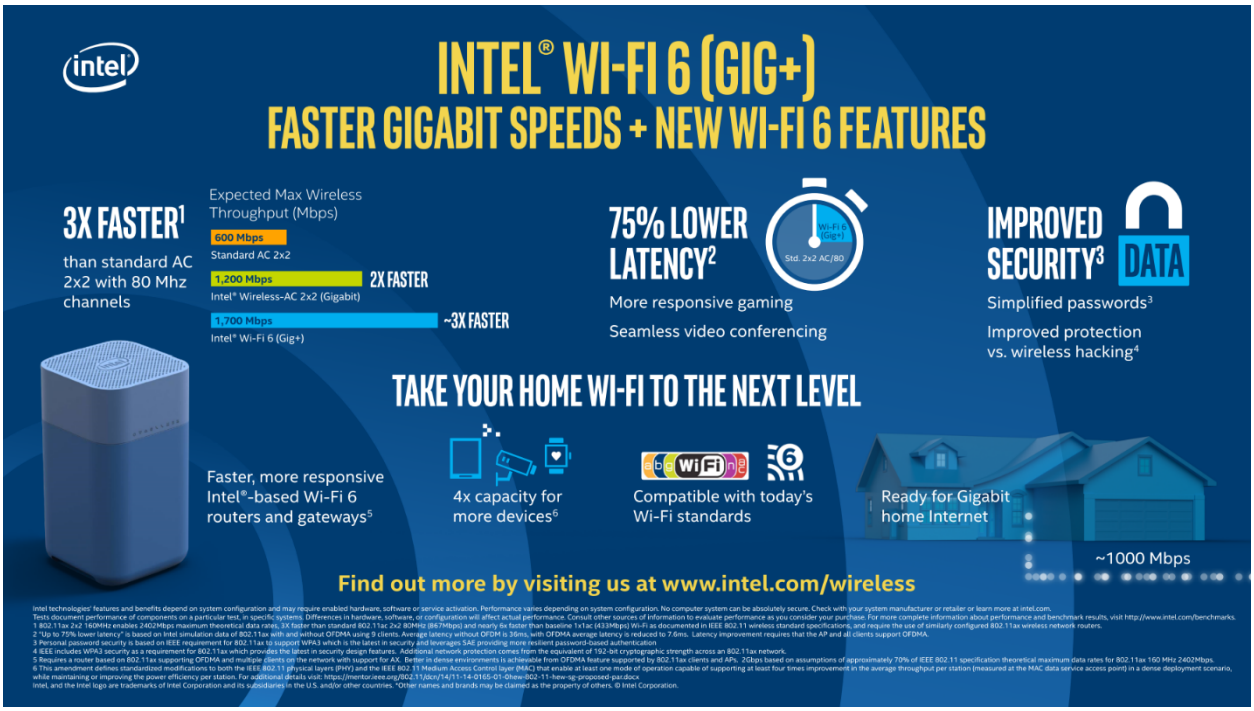
WAV600 Series can deliver multi-Gigabit Wi-Fi speeds to PCs with integrated Gigabit Wi-Fi or Wi-Fi 6 (Gig+) enabling high-quality user experiences" and "These Wi-Fi SoCs are optimized for the AnyWAN™ SoCs and the Puma™ 7 Family to fully offload the wireless traffic with zero CPU utilization.").

41. In addition to its router-side business, Intel has manufactured, used, marketed, sold, offered for sale, and exported from and imported into the United States client-side wireless adapters utilizing the Wi-Fi 6, Wi-Fi 6E, and Wi-Fi 7 wireless standards ("Intel's Accused Adapter Products"). Wi-Fi 6 or 6E, also known as IEEE 802.11ax, is an IEEE standard from the Wi-Fi Alliance, of which Intel is a member. Wi-Fi 7 is also an IEEE standard, otherwise known as IEEE 802.11be. Intel wireless adapters utilizing Wi-Fi 6 or 6E include, but are not limited to, the AX101, AX200, AX201, AX201, AX210, AX211, AX411. Intel wireless adapters utilizing Wi-Fi 7 include, but are not limited to, the BE200 and BE202.

42. Additionally, Intel released Ice Lake, "a new highly-integrated platform for laptops, combining the new 'Sunny Cove' core architecture and the new Gen11 graphics architecture with both Thunderbolt™ 3 and Intel® Wi-Fi 6 (Gig+) integrated for the first time, providing best-in-class connectivity. See https://www.edge-ai-vision.com/2019/05/intel-computex-preview-new-products-deliver-real-world-performance-up-to-2x-gaming-and-8x-ai-boost/. Ice Lake and other processors integrating Intel Wi-Fi 6 (Gig+) ("Intel's Accused Wi-Fi Integrated Processors") simplify the production of connected computers. See e.g. https://www.anandtech.com/show/14514/examining-intels-ice-lake-microarchitecture-and-sunny-cove/9 (describing that the technology "allows Intel's partners to use different antenna 'RF' modules depending on what it wants to support, such as single antenna designs, dual antenna designs, or higher bandwidth mode."). These processors include: Intel's 10th Gen Core

Processors (aka "Ice Lake"), which boast "integrated Wi-Fi 6 (Gig+) (https://www.intel.com/content/www/us/en/products/docs/processors/core/10th-gen-processors.html), including the Core i7, i5, i3, and Pentium 6805 processors; Intel's 11th Gen Core Processors (aka), including the U-Series Laptop Processors, H-35 Laptop Processors, S-Series Desktop Processors, and H-Series Laptop Processors (https://www.intel.com/content/www/us/en/products/docs/processors/core/11th-gen-processors.html), all of which have an integrated Intel Wi-Fi 6 AX201 or an Discrete Intel Killer Wi-Fi 6E AX1675; Intel's 12th Gen Core Processors, which include Intel Wi-Fi 6/6E (Gig+) (https://www.intel.com/content/www/us/en/products/docs/processors/core/12th-gen-processors.html); Intel's 13th Gen Core Mobile Processors, which include Intel Wi-Fi 6E (Gig+) (https://www.intel.com/content/www/us/en/products/docs/processors/core/13th-gen-core-mobile-brief.html); Intel's 14th Gen Core Desktop Processors, which supports discrete Intel Wi-Fi 7(5 Gig) (https://www.intel.com/content/www/us/en/products/docs/processors/core/core-14th-gen-desktop-brief.html); Intel's 14th Gen Core Processors HX-Series, which supports discrete Intel Wi-Fi 7 (5 Gig) and integrated Intel Killer Wi-Fi 6E with Intel Double Connect (https://www.intel.com/content/www/us/en/products/docs/processors/core/core-14th-gen-mobile-brief.html).

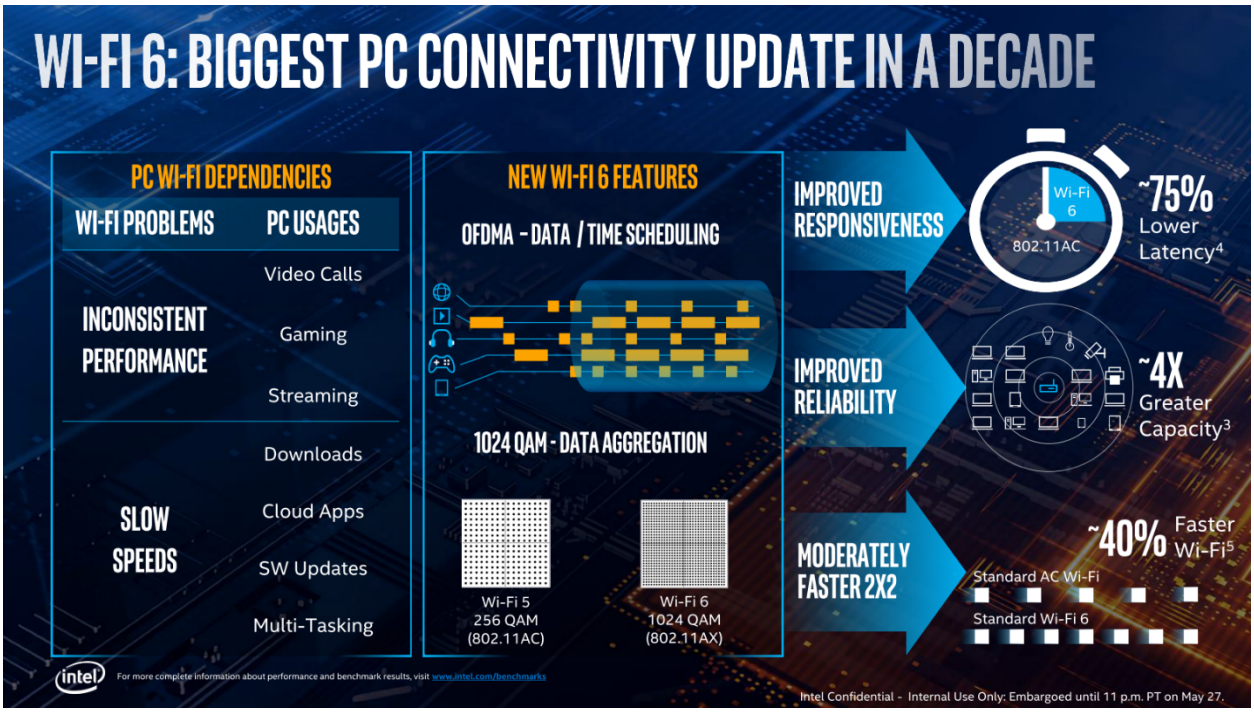
43. At Computex 2019, Intel pushed new Wi-Fi 6 routers from Netgear, TP Link, and Edimax utilizing the Intel® Home Wi-Fi Chipset WAV600 Series, to boost the adoption rate of Wi-Fi 6. See e.g. https://www.notebookcheck.net/Intel-pushing-new-Wi-Fi-6-routers-from-various-manufacturers-to-boost-adoption-rate.422691.0.html. The following is a promotional advertisement, included in Intel's 2019 Computex Press Kit, that touts the benefit of Intel-branded Wi-Fi 6 (Gig+) wireless adapters and Intel® Home Wi-Fi Chipset WAV600 Series:



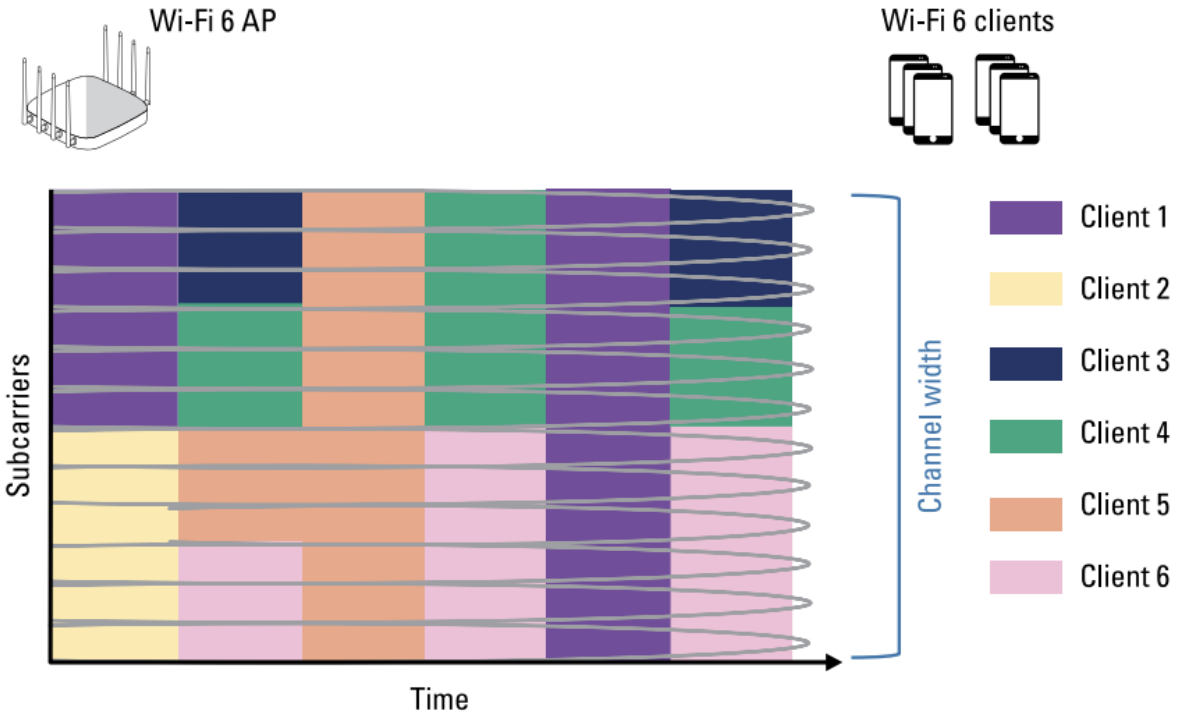
In the lower left portion of the advertisement, Intel described "[f]aster, more responsive Intel-based Wi-Fi 6 routers and gateways".

44. A key feature of Wi-Fi 6 (and later standards like Wi-Fi 7) is orthogonal frequency division multiple access ("OFDMA"). See https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6. OFDMA enables wireless carriers to efficiently utilize their available frequency band by dividing the available band into sub-carriers and the transmission window into timeslots. This allows users to communicate with multiple clients and simultaneously transmit data. Assigning users into subcarriers and timeslots depends on the bandwidth needed by each user as well as other factors, which may include device constraints, quality of service, data loads, or usage patterns, among others. An example of how this works is when two phones send data over the same line. Each phone may be assigned a time interval so that they take turns sending their data at their assigned intervals. However, these time frames are small, making it seem as if both phones are sending their data simultaneously and seamlessly.

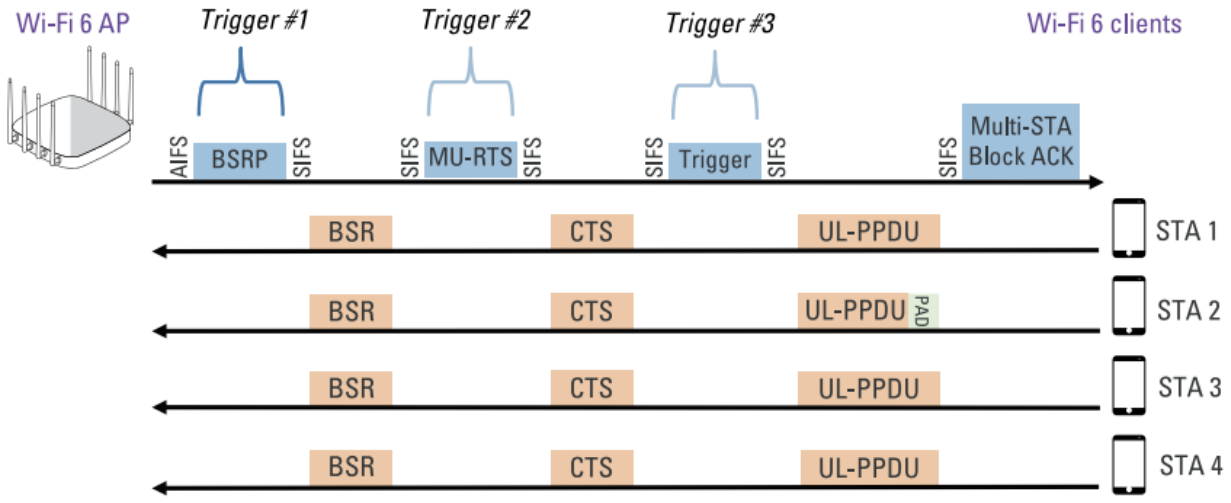
45. Intel pushed hard for the adoption of Wi-Fi 6 and its new OFDMA feature for data/time scheduling. For example, Intel's marketing materials described that Wi-Fi 6 was the biggest PC connectivity update in a decade, as reflecting in the tile of the marketing slide below, which was released on May 27, 2019:



46. A pictorial representation of OFDMA is shown below:



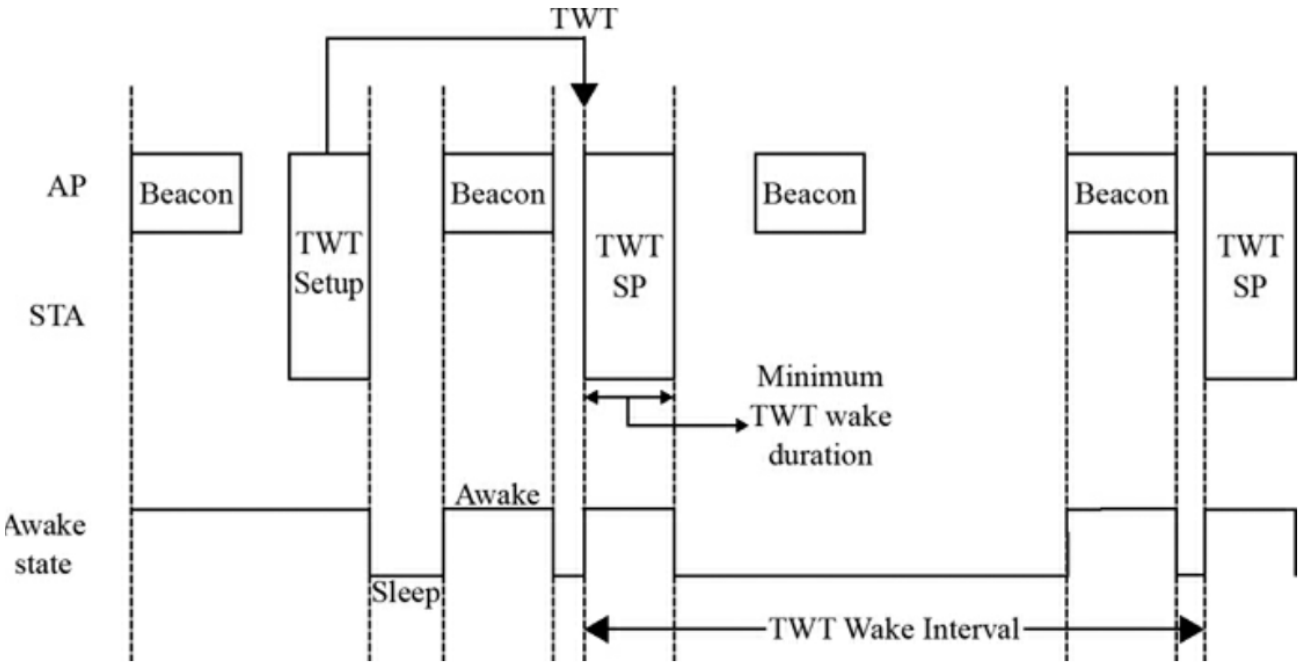
47. As can be seen, 6 cell phones (each represented by a different color) broadcast their data to the Wi-Fi 6 router during one of six timeslots and using one of twelve different subcarriers. The router determines when each device broadcasts and on which subcarrier, the procedure of which is shown below:



48. The router first sends out a buffer status report poll (BSRP) to all devices requesting they report back, among other things, the quality of service (QoS) category of the data each device needs to send. Such information is provided in each device's buffer status report (BSR). After receiving these devices' BSRs, the router determines which timeslot and on which subcarrier each device should transmit their data and then communicates this data using Trigger #3 in the above figure.

49. Wi-Fi 6 and later standards (e.g., Wi-Fi 7) also include target wake time (TWT) as a feature. TWT is a specific time or set of times for individual stations (STAs), such as a laptop, smartphone, or any internet of things device, to awaken in order to exchange frames with other STAs. A STA has a transceiver cycling between an active, or awake, mode in which power is consumed to exchange information, and a sleep mode in which power is conserved.

50. The operation of TWT is shown in the figure below:



51. As shown above, an access point (AP), such as a Wi-Fi 6 router, sends TWT setup information to a STA transceiver (such as on a laptop, phone, or other device) when to switch from sleep mode to active mode. This information is used to set a timer within the device. When the time goes off, at the beginning of each TWT session or service period (TWT SP), the STA wakes up so it can transmit or receive data.

52. As also seen on the figure, the device transceiver is also active during a beacon period. If no beacon is detected, the wi-fi router may have switched the network's channel. To facilitate reconnecting devices that were asleep during a channel switch, Wi-Fi 6 (and later) is configured such that a STA can efficiently move their activity when the absence of a beacon change is noticed. Accordingly, when a STA connects to a network, it receives a future channel guidance element informing it about the likely future channel if the router changes channels of operation. As such, when the transceiver wakes up, it will monitor the first channel for a beacon. If no beacon is detected, it utilizes future channel guidance to increase the channel number to the second likely channel. It will then reset its timer and wait for the next expected transmission from the router.

53. With previous wireless standards, devices were either connected or they were not. Wi-Fi 6 (and later) alternates a transceiver between active and sleep modes, which frees up bandwidth and saves power.

54. Intel's Accused Gateway Products, Intel's Accused Adapter Products, and Intel's Accused Wi-Fi Integrated Processors utilizing Wi-Fi 6 (and later) infringe one or more claims of the 129, 672, 043, and 152 Patents in connection with OFDMA and TWT functionality.

2. Intel 8th Generation (and later) Core Processors

55. Intel is also a member of the Fast Identity Online ("FIDO") Alliance. The FIDO Alliance is an open industry association launched in February 2013 whose stated mission is to develop and promote authentication standards that "help reduce the world's over-reliance on passwords." Intel is also a member of the Trusted Computing Group (TCG), a computer industry consortium that created the TPM standard, which was later adopted by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and subsequently named ISO/IEC 11889.

56. As part of its work in these groups, Intel developed and implements a TPM, or a trusted platform module, which it includes in certain of its microprocessor chips. The TPM is a physical or embedded security technology (microcontroller) that resides on a computer's motherboard or in its processor. TPMs use cryptography to help securely store essential and critical information on PCs to enable platform authentication. They store a variety of sensitive information—such as user credentials, passwords, fingerprints, certificates, encryption keys, or other important consumer documentation—behind a hardware barrier to keep it safe from external attacks.

57. Beginning with Windows 11, Microsoft (also a member of FIDO) required that all PCs running Windows 11 must have a TPM to run the operating system. Intel's latest microprocessors provide this functionality. Intel describes on its website that:

> Trusted platform module (TPM) technology helps keep PCs secure by offering hardware-level protection against malware and sophisticated cyberattacks. TPM technology can be embedded into modern CPUs and "securely store[s] artifacts used to authenticate the

platform." The artifacts TPMs protect range from passwords to certificates to fingerprints—any important information users want securely stored.

https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/trusted-platform-module.html.

58. Accordingly, in providing TPM functionality, Intel actively contributes to infringement of the Patents-in-Suit by providing a component of an infringing product, with knowledge that it is especially made or adapted for use in such infringement, and is not suitable for substantial noninfringing uses. Intel's Core processors, including and later than the 8th generation processors (the "Accused Products 2") such as the Core i7 processor, all include a Trusted Platform Module (TPM) to meet Microsoft Windows 11 requirements.

59. Direct infringement occurs vis a via Microsoft. Specifically, Microsoft directly infringes the 730 Patent by utilizing a universal platform passwordless architecture incorporating an authenticator, including Windows Hello on Windows 10 and 11. This architecture includes the Microsoft Identity platform, which controls the actions of authenticators and the dissemination of tokens and other access messages. This offers users identity and access management services which entail requesting user authentication (without the use of passwords) and receiving tokens in a manner directed and controlled by Microsoft, including the use of Microsoft Authentication Library.

60. Microsoft's password-less architecture verifies a user during authentication of an integrated device, which may be a computer running Windows 11 that includes Windows Hello as a native component. Following user verification via biometrics, the Microsoft Identity platform utilizes FIDO2 and analogous protocols to authenticate the device and OpenID Connect

to permit access to various resources, including Microsoft applications, subscriptions, and services, such as Outlook, Office, Skype, Xbox Live, etc. *See* **Exhibit 16.**

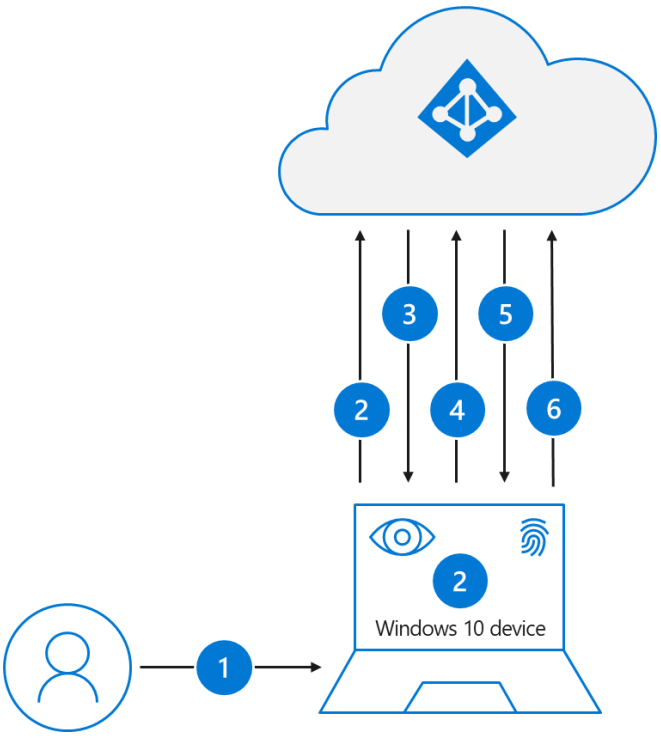
61. Computers running Microsoft Windows persistently store biometric user data. Whether manufactured by Microsoft or its partners, such as Dell, Windows 10 and 11 devices must meet minimum hardware requirements set by Microsoft. *See* **Exhibit 17**. The minimum hardware requirements ensure Windows Hello can utilize specialized hardware and software, such as Virtualization Based Security (VBS) and Trusted Platform Module (TPM) 2.0 to isolate, protect, and secure the channel by which a user's biometric data is communicated. *See* **Exhibit 18.**

62. For example, when a user elects to use facial recognition for authentication, a face template is generated and encrypted using keys only accessible to the VBS, and then stored on disk. *See id.* Accordingly, facial templates are persistently stored on a Windows device's storage. Likewise, these devices persistently store fingerprint data, but do so instead in the sensor's dedicated memory. *See id.* In all cases, the biometric data is stored so as to prevent unauthorized alterations.

63. Authenticators such as Windows Hello must be FIDO2 certified. *See* **Exhibit 19**. FIDO compliant authenticators store biometric data of user in tamper proof format unable to be subsequently altered. Authenticators such as Microsoft Hello, accordingly, stores biometric data in a tamper proof format. Windows Hello stores a device ID code uniquely identifying each integrated device. Microsoft's universal platform passwordless architecture is based on FIDO2. *See* **Exhibit 18**. Instead of passwords, FIDO2 uses public/private key encryption. *See* **Exhibit 16**. The private key is generated and stored on the authenticator, while the public key is sent to the Microsoft Identity platform. *See id.* When a user attempts to authenticate, Microsoft Identity

platform sends a nonce to the authenticator, which is signed with the private key. *See id.* The signed nonce is then returned to the Microsoft Identity Platform and the signature verified with the corresponding public key. For this to work, Microsoft Identity Platform must select the correct public key for the particular authenticator being used. This is accomplished by sending a credential ID indicating which public key to use along with the signed nonce. Accordingly, each public key within Microsoft Identity includes a reference to a credential ID uniquely identifying the device from which it was created. *See* **Exhibit 20**. The credential ID is thus a device ID code that is part of a pair. Being one part of a pair places the Device ID in a tamper proof format on the integrated device.

64. To perform biometric verification of the user, authenticators like Windows Hello causes the device to prompt a user for biometric verification and receive scan data from a biometric scan. In Windows Hello, the prompt for biometric verification occurs after the user dismisses the lock screen, as shown below.

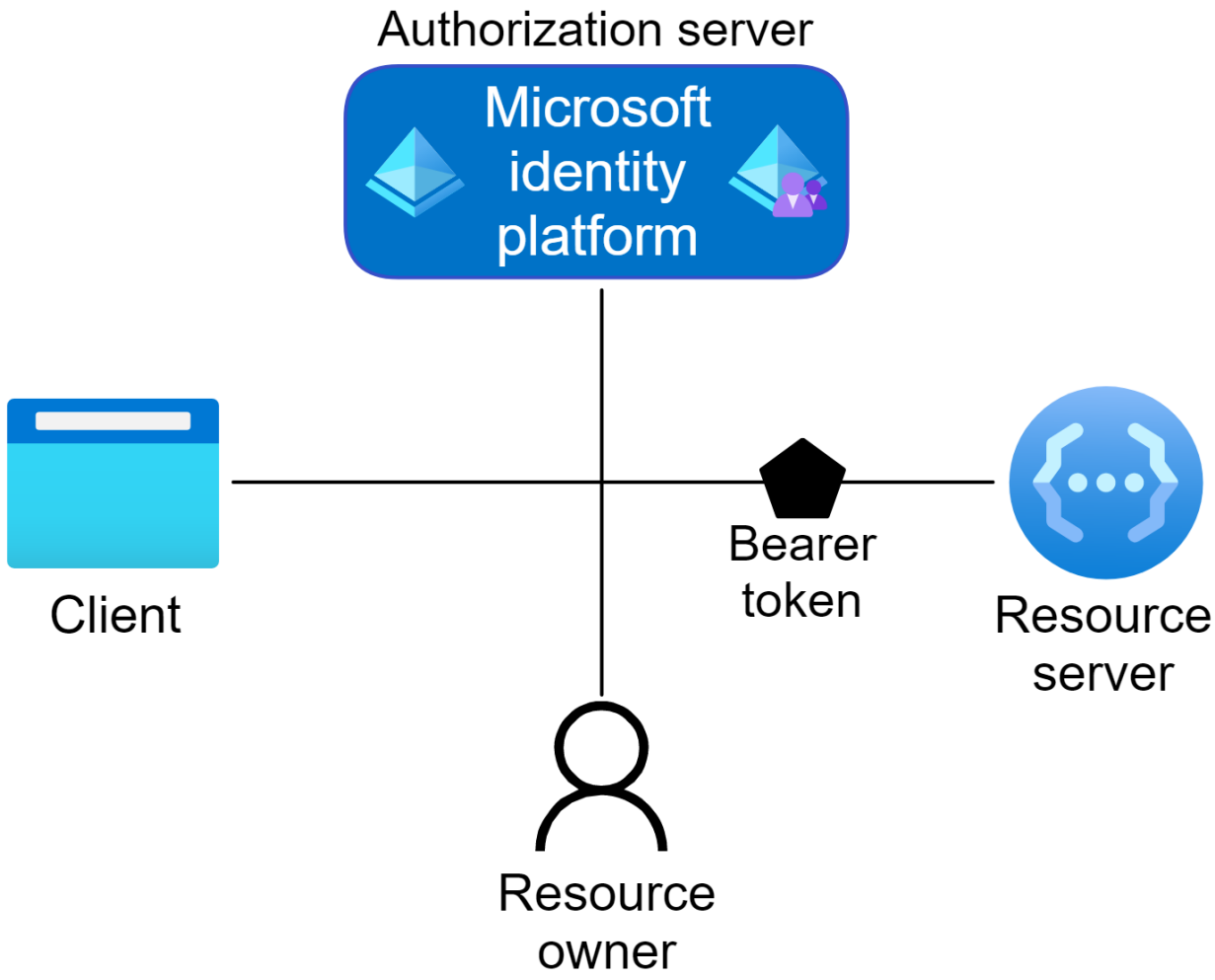


1. A user signs into Windows using biometric or PIN gesture. The gesture unlocks the Windows Hello for Business private key and is sent to the Cloud Authentication security support provider, referred to as the *Cloud AP provider*.
2. The Cloud AP provider requests a nonce (a random arbitrary number that can be used just once) from Azure AD.
3. Azure AD returns a nonce that's valid for 5 minutes.
4. The Cloud AP provider signs the nonce using the user's private key and returns the signed nonce to the Azure AD.
5. Azure AD validates the signed nonce using the user's securely registered public key against the nonce signature. After validating the signature, Azure AD then validates the returned signed nonce. When the nonce is validated, Azure AD creates a primary refresh token (PRT) with session key that is encrypted to the device's transport key and returns it to the Cloud AP provider.
6. The Cloud AP provider receives the encrypted PRT with session key. Using the device's private transport key, the Cloud AP provider decrypts the session key and protects the session key using the device's Trusted Platform Module (TPM).
7. The Cloud AP provider returns a successful authentication response to Windows. The user is then able to access Windows as well as cloud and on-premises applications without the need to authenticate again (SSO).

See **Exhibit 21**.

65. The use of Windows Hello within Microsoft's universal platform password-less architecture is not limited to logging onto a Windows 10/11 computer. For instance, resources, such as applications, services, subscriptions, and websites utilizing the Microsoft Identity Platform for Identity and Access Management natively receive the benefit of utilizing authenticators for password-less user authentication. *See* **Exhibit 22**. As such, the Microsoft Identity Platform permits the use of Microsoft approved authenticators to log into any platform or browser, or confirm any login, with the use of biometric authentication. *See* **Exhibit 23**.

66. Microsoft Identity platform operates as a third party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices (i.e., Microsoft approved authenticators). Microsoft depicts the relationship between the parties involved in authentication and authorization below.



See **Exhibit 24**.

67. Microsoft Identity takes on the role of the authorization server responsible for authenticating the user. *See id.* Instead of using passwords, it utilizes FIDO2 and analogous protocols to authenticate users. *See* **Exhibit 25.**

68. The protocols employed use public/private key encryption. *See* **Exhibit 16**. Each public key is identified by a unique credential ID. As discussed above, the private key is generated and stored on the authenticator and the public key is sent to Microsoft Identity platform. When a user attempts to authenticate, Microsoft Identity platform sends a nonce to the authenticator, which is signed with the authenticator's private key, returned to Microsoft Identity

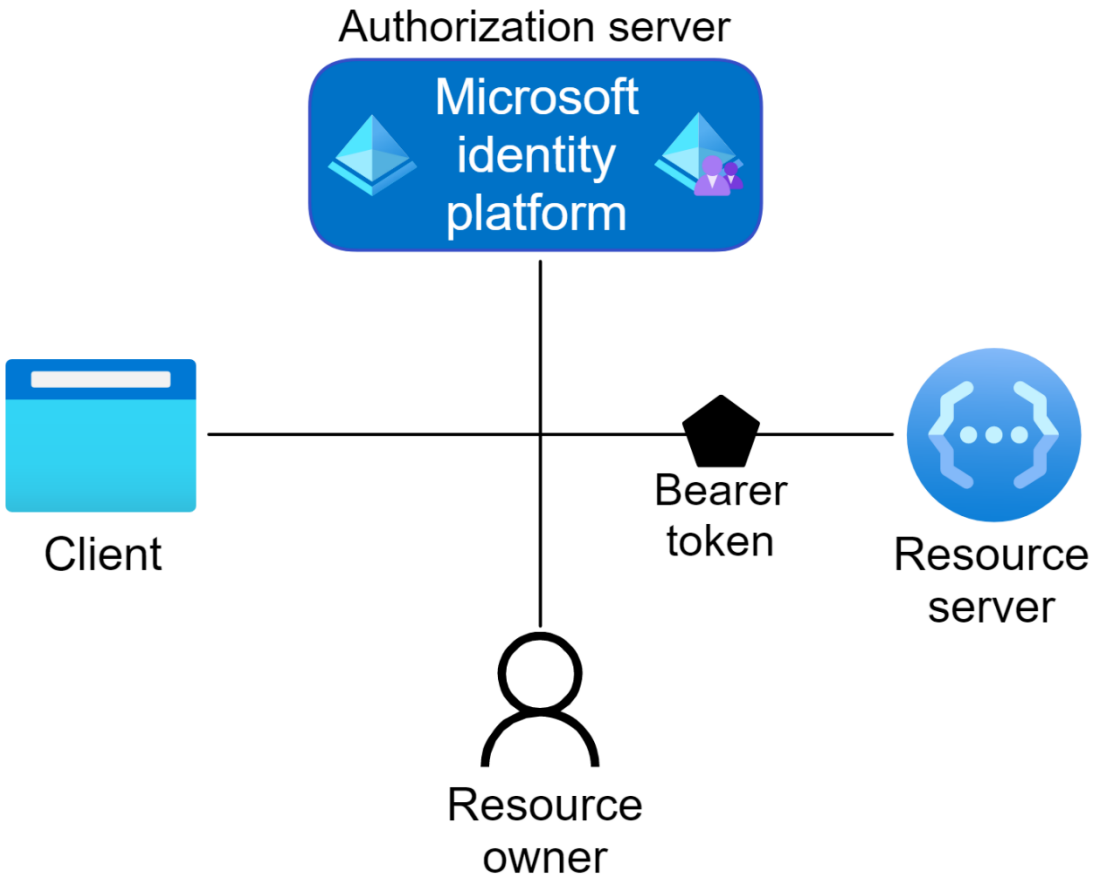
with a credential ID, and verified with the public key held by Microsoft Identity Platform corresponding to the sent credential ID. *See id.* Sending the credential ID with the signed nonce enables Microsoft Identity Platform to select the correct public key for the particular authenticator being used. A user account, therefore, contains a list of "PassportDevices," (i.e., authenticators) which each entry in the list including a "DeviceId" (i.e., credential ID) and a "PublicKey." *See* **Exhibit 26**. Accordingly, each public key within Microsoft Identity includes a reference to the specific device from which it was created and should be used. *See* **Exhibit 20**.

69. Authenticators within Microsoft's universal platform password-less architecture (such as Windows Hello) sign the nonce and return it with the credential ID after a determining that the scan data matches the biometric data. Computers running Windows 10/11 can wirelessly send the device ID code and nonce request via a wireless connection to a local router or mobile phone.

70. Utilizing OAuth 2.0 and OpenID Connect, Microsoft Identity platform issues access messages in the form of Bearer Tokens to various resources. *See* **Exhibit 27**. Acting as an authorization server, Microsoft Identity handles the trust relationship between the parties, including issuing security tokens (i.e., Bearer Tokens) for granting access (authorization) after the user has signed in (authenticated). *See* **Exhibit 20**. The Bearer Token is passed between the parties to assure authentication and grant access. There are four types of tokens issued by Microsoft Identity: Access Tokens, ID Tokens, Refresh Tokens, and Primary Refresh Tokens. *See id.* The type of token issued depends on the resource being accessed. Regardless of the resource, the Bearer Tokens received from Microsoft Identity are used to get access to the resource, which may be an application, website, service, subscription, etc. offered by Microsoft

or businesses and developers subscribing to Microsoft's Identity and Access Management service and are thus "access messages."

71. The issuance of tokens serving as access messages within Microsoft's universal platform password-less architecture is shown in the figure below. As shown, the resource server providing the application, subscription, service, etc. to be accessed is a separate entity from Microsoft Identity Platform. Thus, regardless of whether the resource is one provided by Microsoft or its customers, the resource server is a separate entity. As such, communication between the resource server and Microsoft Identity Platform is required. This communication is accomplished by the resource server sending a request for authentication using URLs provided by Microsoft and in a form dictated by Microsoft. In many instances, the communication will be mediated via a client, such Microsoft Edge or another web browser, Windows Cloud AP, etc. Regardless of the client, upon receipt of the request form the resource server for user authentication, Microsoft Identity Platform sends requests to a Microsoft approved authenticator to verify the user and sign a nonce. Often the client will facilitate this communication between the Microsoft Identity Platform and the authenticator. After receiving and verifying the signature generated by the authenticator, Microsoft Identity Platform issues a bearer token. Receipt of the bearer token by the resource server indicates user authentication by Microsoft Identity Platform acting as a third-party with respect to the resource server.

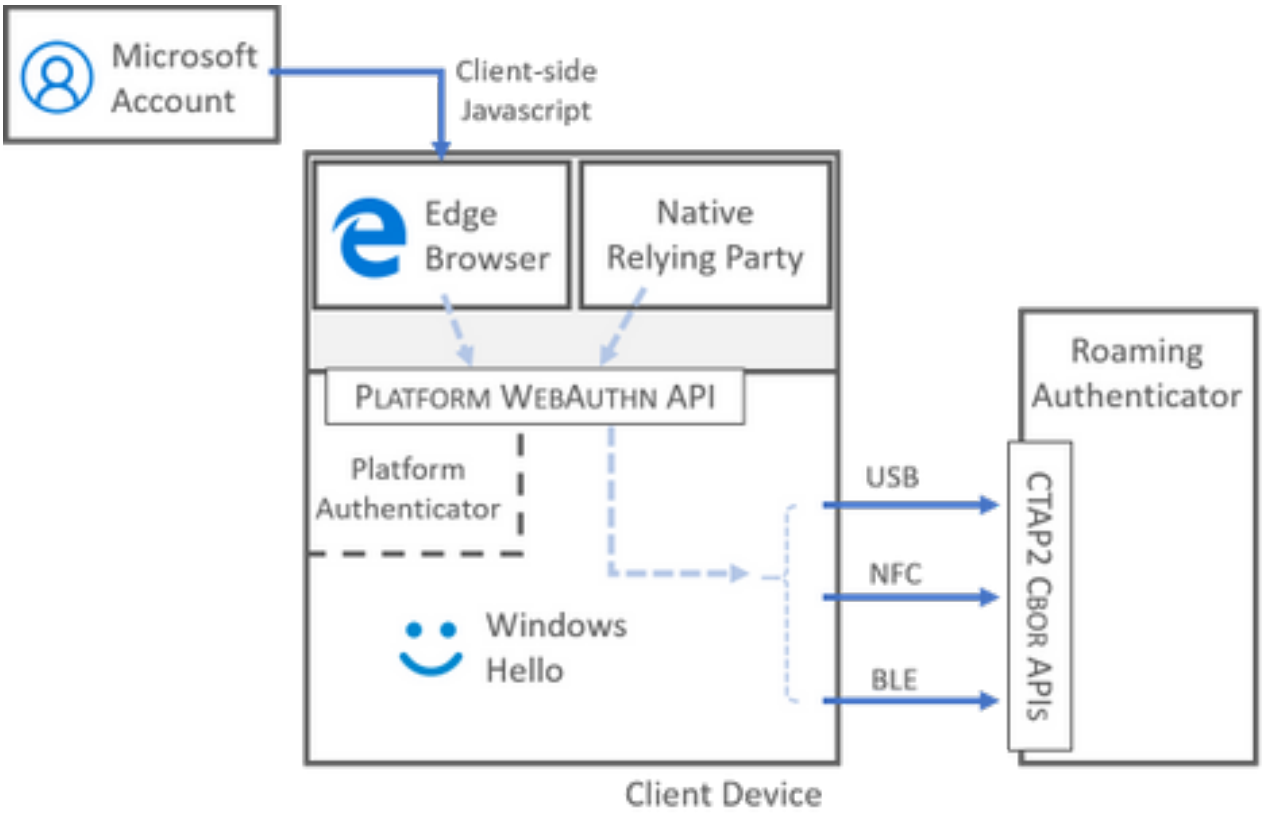


72. As the foregoing shows, Microsoft directly infringes one or more claims of the 730 Patent via the Microsoft Identity Platform at the center of Microsoft's universal platform password-less architecture, using Windows Hello as an authenticator.

73. As discussed above, Intel Core 8th generation and later processors include a TPM to meet Windows 11 TPM requirements. A TPM is an embedded security technology that resides in a computer's motherboard or processor and uses cryptography to securely store sensitive information to enable platform authentication, including biometric information and encryption keys. Windows 11 TPM requirements enables the Windows Hello implementation of FIDO.

74. A core component of FIDO is WebAuthn. FIDO2: Web Authentication (WebAuthn) - FIDO Alliance ("Web Authentication (WebAuthn), a core component of FIDO

Alliance's FIDO2 set of specifications, is a web-based API that allows websites to update their login pages to add FIDO-based authentication on supported browsers and platforms."); *see also* WebAuthn APIs - Windows Security | Microsoft Learn ("Microsoft has long been a proponent of passwordless authentication, and has introduced the W3C/Fast IDentity Online 2 (FIDO2) Win32 WebAuthn platform APIs in Windows 10 (version 1903)."). A variety of the functionality of FIDO is performed by an authenticator. Web Authentication: An API for accessing Public Key Credentials - Level 2 (w3.org) ("Authenticator / WebAuthn Authenticator A cryptographic entity, existing in hardware or software, that can register a user with a given Relying Party and later assert possession of the registered public key credential, and optionally verify the user, when requested by the Relying Party."); *see also* FIDO Technical Glossary (fidoalliance.org) ("A FIDO Authenticator is responsible for user verification, and maintaining the cryptographic material required for the relying party authentication."). A TPM, as included in Intel Core 8th generation and later processors, is a specific instance of an authenticator called a platform authenticator. Web Authentication: An API for accessing Public Key Credentials - Level 2 (w3.org) ("Implementing compliant authenticators is possible in … (b) on an on-device Secure Execution Environment, ***Trusted Platform Module (TPM)***, or a Secure Element (SE)... Authenticators being implemented on device are called ***platform authenticators***."). A component of Windows Hello is a platform authenticator, making the TPM in Intel Core 8th generation and later processors a part of Windows Hello in Windows 11 PCs.



75. As shown in the above figure, the WebAuthn API is utilized to make requests to Windows Hello and the Platform Authenticator (i.e., the TPM in Intel Core 8th generation and later processors). Servicing these requests requires the firmware in these processors be capable of interfacing with the WebAuthn API. As such, Intel Core 8th generation and later desktop processors are a material part of the invention claimed in the 730 Patent and especially adapted for use in Windows Hello and thus infringe one or more claims of the 730 Patent.

76. The Accused Products are not suitable for substantial non-infringing uses. Currently, Intel Core 8th generation and later processors are marketed exclusively for use with Windows. Apple uses their own proprietary processors in their computers, leaving Windows computers as the only home for Intel 8th generation and later processors.

77. Accordingly, Intel Core processors including and later than the 8th generation contributorily infringe one or more claims of the 730 Patent.

78. Proxense has at all times complied with the marking provisions of 35 U.S.C. § 287 with respect to the Patents-in-Suit. On information and belief, any prior assignees and licensees have also either complied with the marking provisions of 35 U.S.C. § 287, or else were excused from the obligation to mark for the reason that § 287 does not apply.

CLAIM 1
(Infringement of the 129 Patent)

79. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

80. Proxense has not licensed or otherwise authorized Intel to make, use, offer for sale, sell, or import any products that embody the inventions of the 129 Patent.

81. Defendant infringes at least claims 1, 16, and 18 of the 129 Patent in violation of 35 U.S.C. § 271(a) with respect to the Intel's Accused Gateway Products, Intel's Accused Adapter Products, and Intel's Accused Wi-Fi Integrated Processors. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

82. For example, Defendant directly infringe at least claims 1, 16, and 18 of the 129 Patent by making, using (*e.g.*, performing/executing), selling, and/or offering to sell the Intel's Accused Gateway Products, Intel's Accused Adapter Products, and Intel's Accused Wi-Fi Integrated Processors within the United States. A key feature of Wi-Fi 6 and later standards is OFDMA, which divides the available frequency band into subcarriers and the transmission window into timeslots. Assigning users into subcarriers and timeslots depends on the bandwidth needed by each user as well as other factors, which may include device constraints, quality of service, data loads, or usage patterns, among others. In a Wi-Fi 6 or later network, devices on that network broadcast their data to the wireless router. The router first sends out a buffer status

report poll (BSRP) to all devices requesting they report back, among other things, the quality of service (QoS) category of the data each device needs to send. Such information is provided in each device's buffer status report (BSR). After receiving these devices' BSRs, the router determines which timeslot and on which subcarrier each device should transmit their data. Exemplary claim charts are included herewith as **Exhibit 6**.

83. Defendant received actual notice of the 129 Patent at least as early as the filing of this Complaint. Defendant performed and continue to perform the acts that constitute infringement, with knowledge or willful blindness that the acts would constitute infringement of the 129 Patent.

84. Defendant do so knowingly and with intent to commit these infringing acts. Defendant also continue to make, use, offer for sale, sell, and/or import the accused products, despite their knowledge of the 129 Patent, thereby specifically intending to infringe the 129 Patent.

85. Proxense has been injured and seeks damages to adequately compensate it for Intel's infringement of the 129 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

86. Upon information and belief, Intel will continue to infringe the 129 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 129 Patent by Intel.

CLAIM 2
(Infringement of the 672 Patent)

87. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

88. Proxense has not licensed or otherwise authorized Intel to make, use, offer for sale, sell, or import any products that embody the inventions of the 672 Patent.

89. Defendant infringes at least claim 1 of the 672 Patent in violation of 35 U.S.C. § 271(a) with respect to the Intel's Accused Gateway Products, Intel's Accused Adapter Products, and Intel's Accused Wi-Fi Integrated Processors. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

90. For example, Defendant directly infringe at least claim 1 of the 672 Patent by making, using (*e.g.*, performing/executing), selling, and/or offering to sell the Intel's Accused Gateway Products, Intel's Accused Adapter Products, and Intel's Accused Wi-Fi Integrated Processors within the United States. A key feature of the Wi-Fi 6 and later standards is OFDMA, which divides the available frequency band into subcarriers and the transmission window into timeslots. Assigning users into subcarriers and timeslots depends on the bandwidth needed by each user as well as other factors, which may include device constraints, quality of service, data loads, or usage patterns, among others. In a Wi-Fi 6 or later network, devices on that network broadcast their data to the wireless router. The router first sends out a buffer status report poll (BSRP) to all devices requesting they report back, among other things, the quality of service (QoS) category of the data each device needs to send. Such information is provided in each device's buffer status report (BSR). After receiving these devices' BSRs, the router determines which timeslot and on which subcarrier each device should transmit their data. Exemplary claim charts are included herewith as **Exhibit 7**.

91. Defendant received actual notice of the 672 Patent at least as early as the filing of this Complaint. Defendants performed and continue to perform the acts that constitute

infringement, with knowledge or willful blindness that the acts would constitute infringement of the 672 Patent.

92. Defendant do so knowingly and with intent to commit these infringing acts. Defendants also continues to make, use, offer for sale, sell, and/or import the accused products, despite their knowledge of the 672 Patent, thereby specifically intending to infringe the 672 Patent.

93. Proxense has been injured and seeks damages to adequately compensate it for Intel's infringement of the 672 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

94. Upon information and belief, Intel will continue to infringe the 672 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 672 Patent by Intel.

CLAIM 3
(Infringement of the 043 Patent)

95. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

96. Proxense has not licensed or otherwise authorized Intel to make, use, offer for sale, sell, or import any products that embody the inventions of the 043 Patent.

97. Defendant infringe at least claim 1 of the 043 Patent in violation of 35 U.S.C. § 271(a) with respect to the I Intel's Accused Gateway Products, Intel's Accused Adapter Products, and Intel's Accused Wi-Fi Integrated Processors. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

98. For example, Defendant directly infringe at least claim 1 of the 043 Patent by making, using (*e.g.*, performing/executing), selling, and/or offering to sell the Intel's Accused Gateway Products, Intel's Accused Adapter Products, and Intel's Accused Wi-Fi Integrated Processors within the United States. A key feature of the Wi-Fi 6 and later standards is OFDMA, which divides the available frequency band into subcarriers and the transmission window into timeslots. Assigning users into subcarriers and timeslots depends on the bandwidth needed by each user as well as other factors, which may include device constraints, quality of service, data loads, or usage patterns, among others. In a Wi-Fi 6 or later network, devices on that network broadcast their data to the wireless router. The router first sends out a buffer status report poll (BSRP) to all devices requesting they report back, among other things, the quality of service (QoS) category of the data each device needs to send. Such information is provided in each device's buffer status report (BSR). After receiving these devices' BSRs, the router determines which timeslot and on which subcarrier each device should transmit their data. Exemplary claim charts are included herewith as **Exhibit 8**.

99. Defendant received actual notice of the 043 Patent at least as early as the filing of this Complaint. Defendant performed and continue to perform the acts that constitute infringement, with knowledge or willful blindness that the acts would constitute infringement of the 043 Patent.

100. Defendant do so knowingly and with intent to commit these infringing acts. Defendants also continue to make, use, offer for sale, sell, and/or import the accused products, despite its knowledge of the 043 Patent, thereby specifically intending to infringe the 043 Patent.

101. Proxense has been injured and seeks damages to adequately compensate it for Intel's infringement of the 043 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

102. Upon information and belief, Intel will continue to infringe the 043 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 043 Patent by Intel.

CLAIM 4
(Infringement of the 152 Patent)

103. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

104. Proxense has not licensed or otherwise authorized Intel to make, use, offer for sale, sell, or import any products that embody the inventions of the 152 Patent.

105. Defendant infringe at least claims 1 and 7 of the 152 Patent in violation of 35 U.S.C. § 271(a) with respect to the Intel's Accused Gateway Products, Intel's Accused Adapter Products, and Intel's Accused Wi-Fi Integrated Processors. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

106. For example, Defendant directly infringes at least claims 1 and 7 of the 152 Patent by making, using (*e.g.*, performing/executing), selling, and/or offering to sell the Intel's Accused Gateway Products, Intel's Accused Adapter Products, and Intel's Accused Wi-Fi Integrated Processors within the United States. A key feature of the Wi-Fi 6 and later standards is target wake time (TWT), which is a specific time or set of times for individual stations (STAs), such as a laptop, smartphone, or other device, to awaken in order to exchange frames with other STAs. A STA has a transceiver cycling between an active and a sleep mode. An access point (AP),

such as a wireless router, sends TWT setup information to a STA transceiver when to switch from sleep mode to active mode. This information is used to set a timer within the device. When the time goes off, at the beginning of each TWT session or service period (TWT SP), the STA wakes up so it can transmit or receive data. The device transceiver is also active during a beacon period. If no beacon is detected, the wi-fi router may have switched the network's channel. To facilitate reconnecting devices that were asleep during a channel switch, Wi-Fi 6 (and later) is configured such that a STA can efficiently move their activity when the absence of a beacon change is noticed. Accordingly, when a STA connects to a network, it receives a future channel guidance element informing it about the likely future channel if the router changes channels of operation. As such, when the transceiver wakes up, it will monitor the first channel for a beacon. If no beacon is detected, it utilizes future channel guidance to increase the channel number to the second likely channel. It will then reset its timer and wait for the next expected transmission from the router.

107. Exemplary claim charts are included herewith as **Exhibit 9**.

108. Defendant received actual notice of the 152 Patent at least as early as the filing of this Complaint. Defendant performed and continue to perform the acts that constitute infringement, with knowledge or willful blindness that the acts would constitute infringement of the 152 Patent.

109. Defendant do so knowingly and with intent to commit these infringing acts. Defendant also continue to make, use, offer for sale, sell, and/or import the accused products, despite its knowledge of the 152 Patent, thereby specifically intending to infringe the 152 Patent.

110. Proxense has been injured and seeks damages to adequately compensate it for Intel's infringement of the 152 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

111. Upon information and belief, Intel will continue to infringe the 152 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 152 Patent by Intel.

CLAIM 5
(Infringement of the 730 Patent)

112. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

113. Proxense has not licensed or otherwise authorized Intel to make, use, offer for sale, sell, or import any products that embody the inventions of the 730 Patent.

114. Intel contributorily infringes at least claim 1 of the 730 Patent in violation of 35 U.S.C. § 271(c) with respect to the Accused Products 2 by selling or offering to sell in the United States, or importing into the United States, the Accused Products 2 with knowledge that they are especially designed or adapted to operate in a manner that infringes the 730 Patent and despite the fact that the infringing technology or aspects of the products are not a staple article of commerce suitable for substantial non-infringing use.

115. For example, Microsoft's password-less architecture centered around Microsoft Identity and utilizing the Windows Hello authenticator directly infringes at least claim 1 of the 730 Patent, meeting each limitation literally, and, to the extent a limitation is not met literally, under the doctrine of equivalents. Intel's 8th generation and later processors, the Accused Products 2, is a core and material part of the invention as they are built with a TPM to meet Windows 11 requirements. These TPM requirements enable the Windows Hello implementation

of FIDO and thus practicing the claimed invention of the 730 Patent. Intel knew of the 730 patent and that this component was being combined to infringe one or more claims of the patent. Further, the component has no substantial noninfringing uses as Intel 8th generation and later processors are only used on Windows computers.

116. Exemplary claim charts are included herewith as **Exhibit 10**.

117. Intel received actual notice of the 730 Patent at least as early as the filing of this Complaint. Intel performed and continues to perform the acts that constitute indirect infringement, with knowledge or willful blindness that the acts would constitute indirect infringement of the 730 Patent.

118. Intel does so knowingly and with intent to commit these infringing acts. Intel also continues to make, use, offer for sale, sell, and/or import the Accused Products 2, despite its knowledge of the 730 Patent, thereby specifically intending to infringe the 730 Patent.

119. Proxense has been injured and seeks damages to adequately compensate it for Intel's infringement of the 730 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

120. Upon information and belief, Intel will continue to infringe the 730 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 730 Patent by Intel.

DEMAND FOR JURY TRIAL

Plaintiff hereby requests a jury trial of all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief against Defendant as follows:

a. Entry of judgment declaring that Defendant infringes one or more claims of each of the Patents-in-Suit;

b. Entry of judgment declaring that Defendant's infringement of the Patents-in-Suit is willful;

c. An order awarding damages sufficient to compensate Plaintiff for Defendant's infringement of the Patents-in-Suit, but in no event less than a reasonable royalty, including supplemental damages post-verdict, together with pre-judgment and post-judgment interest and costs;

d. Enhanced damages pursuant to 35 U.S.C. § 284;

e. Entry of judgment declaring that this case is exceptional and awarding Plaintiff its costs and reasonable attorney fees pursuant to 35 U.S.C. § 285;

f. An accounting for acts of infringement;

g. Such other equitable relief which may be requested and to which the Plaintiff is entitled; and

h. Such other and further relief as the Court deems just and proper.

Dated: May 23, 2024

Respectfully submitted,

/s/ David L. Hecht
David L. Hecht (**Lead Counsel**)
dhecht@hechtpartners.com
Maxim Price (*pro hac vice* forthcoming)
mprice@hechtpartners.com
Yi Wen Wu (*pro hac vice* forthcoming)
wwu@hechtpartners.com
Tremayne Norris (*pro hac vice* forthcoming)
tnorris@hechtpartners.com

HECHT PARTNERS LLP
125 Park Avenue, 25th Floor
New York, New York 10017
Telephone: (212) 851-6821

Counsel for Plaintiff Proxense, LLC