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

CARBYNE BIOMETRICS, LLC, **Plaintiff,** **vs.** **APPLE INC.,** **Defendant.**	**Civil Action No. 1:23-cv-00324** **JURY TRIAL**

PLAINTIFF'S ORIGINAL COMPLAINT

Plaintiff Carbyne Biometrics, LLC ("Carbyne") files this Complaint for Patent Infringement against Apple Inc. ("Apple") and alleges as follows:

NATURE OF THE CASE

1. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. § 1 *et seq*.

2. Apple has infringed and continues to infringe at least one claim of U.S. Patent Nos. 10,929,512 ("the '512 Patent"); 11,475,105 ("the '105 Patent"); 11,514,138 ("the '138 Patent") (collectively the "Authentication Patents"); 9,972,010 ("the '010 Patent"); 10,713,656 ("the '656 Patent"); and 11,526,886 ("the '886 Patent") (collectively the "Fraud Reduction Patents") (the Authentication and Fraud Reduction Patents are collectively referred to as the "Asserted Patents"). *See* Exs. A-F.

3. Apple infringes directly, literally and/or by the doctrine of equivalents, and/or induces infringement of the Asserted Patents by developing, making, using, selling, offering for

sale, and/or importing into the United States products that incorporate Carbyne's patented authentication and fraud-reducing technology.

4. Carbyne seeks damages and other relief for Apple's infringement of Carbyne's patented technology.

PARTIES

5. Plaintiff Carbyne Biometrics, LLC is a Delaware limited liability company having its principal place of business at 7 East 20th Street #12F, New York, NY 10003.

6. Apple is a corporation organized under the laws of the State of California, having its principal place of business at 1 Apple Park Way in Cupertino, California 95014.

7. Apple maintains various regular and established places of business within the Western District of Texas including: (1) offices at its two Austin campuses located at 12545 Riata Vista Circle, Austin, Texas 78727 and 6900 W Parmer Lane, Austin, Texas 78729; (2) a manufacturing facility in Austin; (3) an engineering center at 320 S. Capital of Texas Hwy, West Lake Hills, Texas 78746; and (4) retail stores located at 2901 S. Capital of Texas Highway, Austin, Texas 78746 ("Apple Barton Creek"), 3121 Palm Way, Austin, Texas 78758 ("Apple Domain Northside"), and 7400 San Pedro Avenue, San Antonio, Texas 78216 ("Apple North Star").

8. On information and belief, Apple develops, makes, uses, imports, offers for sale, and/or sells in Texas and the Western District of Texas devices such as iPhones, iPads, Mac Pros, Mac Studios, iMacs, Mac Minis, MacBook Air laptops, and MacBook Pro laptops that infringe the Asserted Patents.

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

JURISDICTION AND VENUE

9. This is an action for patent infringement under 35 U.S.C. § 271. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a) because this action arises under the patent laws of the United States.

10. This Court has personal jurisdiction over Apple. Apple has done and continues to do business in the State of Texas. Apple has, directly or through subsidiaries or intermediaries, purposefully and voluntarily placed its infringing products and/or services into the stream of commerce with the specific intention and expectation that it's infringing products and/or services will be purchased and used by consumers in Texas and this District. In doing so, Apple has established minimum contacts in Texas such that the exercise of jurisdiction over Apple would not offend traditional notions of fair play and substantial justice as required to satisfy constitutional requirements of due process.

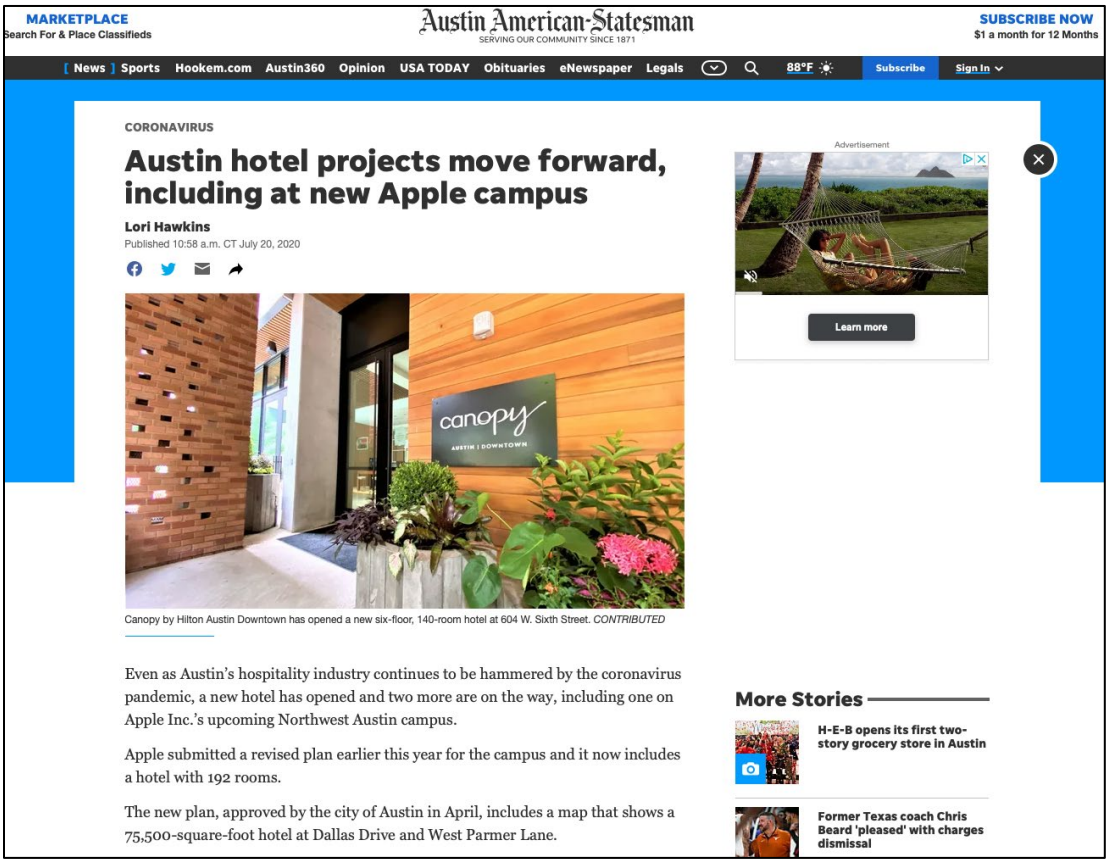
11. Venue is proper in this Court pursuant to 28 U.S.C. § 1400(b) because Apple has committed, and continues to commit, acts of infringement in this District and has regular and established places of business in this District.

12. Apple's presence in this District is substantial. Apple's Austin campuses comprise Apple's second largest hub in the United States and are responsible for running all of Apple's business operations in the Western Hemisphere, including finance, human resources, corporate sales, customer support, information systems, and accounting.[1] Apple's original Austin campus

[1] Lori Hawkins, "*Apple dives deeper into Austin's talent pool*" Austin American-Statesman, (Sept. 7, 2016), https://www.statesman.com/story/news/2016/09/07/apple-dives-deeper-into-austins-talent-pool/10173792007/.

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

at Riata Vista Circle, completed in 2016, consists of 1.1 million square feet of office space.[2] In 2022, Apple completed construction on a new $1 billion campus at 6900 Parmer Lane in Austin. Apple's new Austin campus consists of 3 million square feet of office space on 138 acres and will "initially house 5,000 employees, with the capacity to grow to 15,000."[3] The new campus even includes a 192-room hotel for Apple employees.



MARKETPLACE
Search For & Place Classifieds

Austin American-Statesman
SERVING OUR COMMUNITY SINCE 1871

SUBSCRIBE NOW
$1 a month for 12 Months

[News] Sports Hookem.com Austin360 Opinion USA TODAY Obituaries eNewspaper Legals 88°F Subscribe Sign In

CORONAVIRUS

Austin hotel projects move forward, including at new Apple campus

Lori Hawkins
Published 10:58 a.m. CT July 20, 2020

Canopy by Hilton Austin Downtown has opened a new six-floor, 140-room hotel at 604 W. Sixth Street. *CONTRIBUTED*

Even as Austin's hospitality industry continues to be hammered by the coronavirus pandemic, a new hotel has opened and two more are on the way, including one on Apple Inc.'s upcoming Northwest Austin campus.

Apple submitted a revised plan earlier this year for the campus and it now includes a hotel with 192 rooms.

The new plan, approved by the city of Austin in April, includes a map that shows a 75,500-square-foot hotel at Dallas Drive and West Parmer Lane.

Advertisement
Learn more

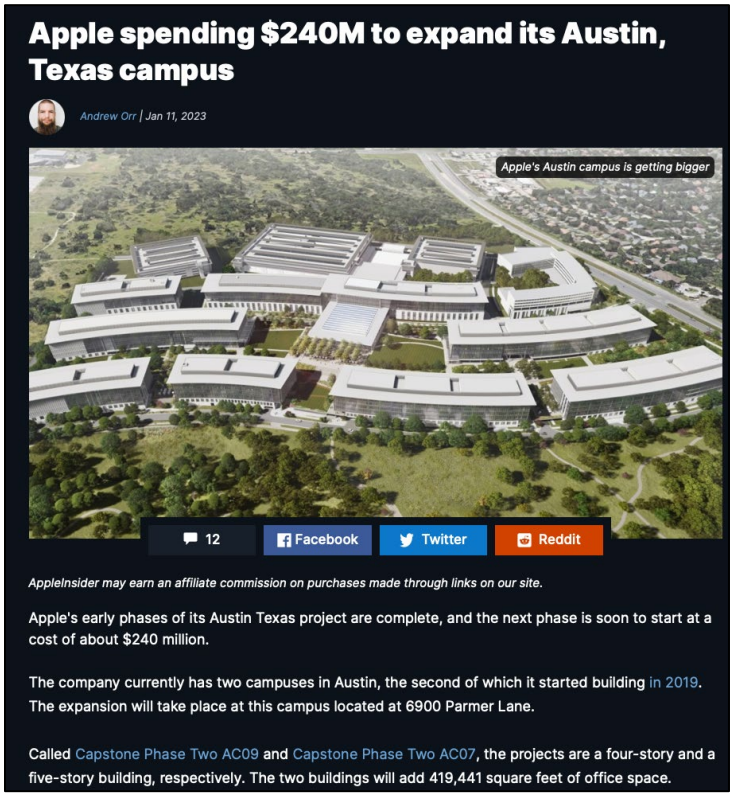
More Stories
H-E-B opens its first two-story grocery store in Austin
Former Texas coach Chris Beard 'pleased' with charges dismissal

Lori Hawkins, *Austin hotel projects move forward, including at new Apple campus*, Austin American-Statesman (July 20, 2020), https://www.statesman.com/story/news/coronavirus/2020/07/20/austin-hotel-projects-move-forward-including-at-new-apple-campus/113737258/.

---

[2] Don Reisinger, *Where Apple Has Quietly Built Its Biggest Campus*, Fortune (Sept. 1, 2016), https://fortune.com/2016/09/01/apple-austin-campus/.
[3] Apple, *Apple expands in Austin* (Nov. 20, 2019), https://www.apple.com/newsroom/2019/11/apple-expands-in-austin/.

13. In early 2023, Apple also announced plans for a $240-million expansion of its new campus to add 419,441 square feet of office space.



Apple spending $240M to expand its Austin, Texas campus

Andrew Orr | Jan 11, 2023

Apple's Austin campus is getting bigger

12 Facebook Twitter Reddit

AppleInsider may earn an affiliate commission on purchases made through links on our site.

Apple's early phases of its Austin Texas project are complete, and the next phase is soon to start at a cost of about $240 million.

The company currently has two campuses in Austin, the second of which it started building in 2019. The expansion will take place at this campus located at 6900 Parmer Lane.

Called Capstone Phase Two AC09 and Capstone Phase Two AC07, the projects are a four-story and a five-story building, respectively. The two buildings will add 419,441 square feet of office space.

Andrew Orr, *Apple spending $240M to expand its Austin, Texas campus*, Apple Insider (Jan. 11, 2023), https://appleinsider.com/articles/23/01/11/apple-spending-240m-to-expand-its-austin-texas -campus.

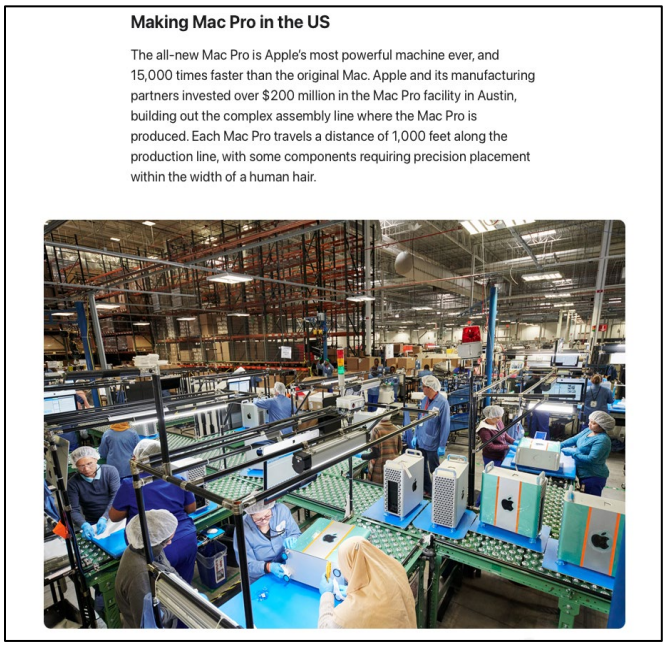
14. Along with its sprawling campuses, Apple operates a seven-story engineering center in the Capital Ridge area of the Austin suburbs.[4] As of 2016, Apple employed around 500 engineers at its Capital Ridge center with a goal of increasing that number to 1,000.[5] The engineers at the Capital Ridge center design and develop both hardware and software.[6] On the

---

[4] Parimal M. Rohit, *Apple buys Austin office building on Capital of Texas Hwy*, Austin Business Journal (Aug. 25, 2021), https://www.bizjournals.com/austin/news/2021/08/25/apple-buys-capital-ridge-austin.html.
[5] *Id.*
[6] *Id.*

hardware front, Apple engineers at Capital Ridge play a major role in developing Apple's A-Series processors (used in the accused products) and other Apple products.[7] In fact, Apple's senior vice president for hardware technologies described the engineers at the Capital Ridge center as "one of [Apple's] most important engineering groups," noting that "[t]hey play a very critical and integral role—they are designing chips that go into all the devices we sell."[8]

15. In addition, the Mac Pro, a product that infringes the Authentication Patents, has been manufactured and/or assembled in Austin for almost five years. According to Apple's CEO Tim Cook, "[b]uilding Apple's most powerful Mac ever in Austin is a testament to the enduring power of American ingenuity and we're proud it's made here."



Apple, *Apple expands in Austin* (Nov. 20, 2019), https://www.apple.com/newsroom/2019/11/apple-expands-in-austin/;

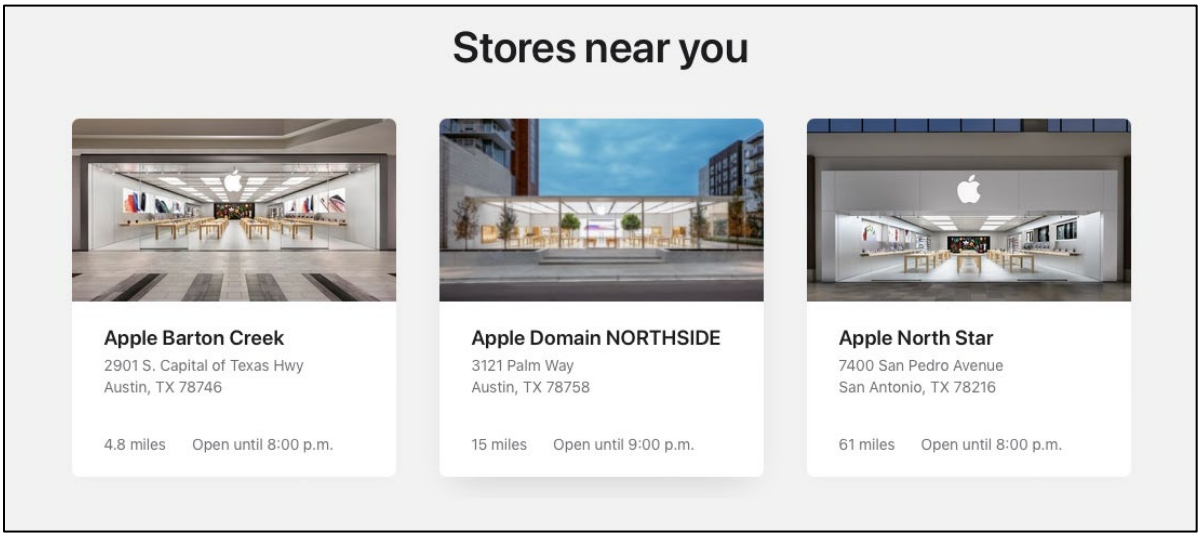
@tim_cook, Twitter (Nov. 20, 2019, 7:15 AM), https://twitter.com/tim_cook/status/1197141315064086530?lang=en.

---

[7] Reisinger, *supra* note 2.
[8] Hawkins, *supra* note 1.

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

16. Apple also operates retail establishments in the District, including retail stores at the Barton Creek Mall and the Domain Northside in Austin, Texas where products that infringe the Asserted Patents are sold, demonstrated, and explained to consumers in this District.



Apple, *Find a Store*, https://www.apple.com/retail/ (last visited Feb. 23, 2023).

17. In total, Apple employs around 7,000 people across its entire Austin footprint.[9] Apple also currently employs several individuals in the Austin metro area who likely have knowledge relevant to Apple's infringement of the Asserted Patents. At least four individuals in Austin have significant, known involvement in the design and architecture of the Secure Enclave.

18. Gilbert Herbeck, "a design engineer who works on the design specifications for Secure Enclave[,]" is "based in Apple's Austin office at Capital Ridge."[10] Mr. Herbeck is "the

[9] Apple, *Apple expands in Austin* (Nov. 20, 2019), https://www.apple.com/newsroom/2019/11/apple-expands-in-austin/.
[10] *Identity Security LLC v. Apple, Inc.*, No. 6:21-CV-00460-ADA, Dkt. No. 55, at 7 (W.D.Tex. Jan. 20, 2022)(Albright, J.)(granting motion to transfer to Austin division).

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

'lead designer and the lead spec author' of Secure Enclave[.]"[11] Sangwan Kim, also at Capital Ridge, "works on certain portions of the specifications for the Secure Enclave."[12]

19. Vincent Pierre Le Roy and Eric Peeters work at the CityView engineering campus "defining security architecture specifications for the Secure Enclave processor."[13]

20. Additionally, Apple currently employs in the Austin metro area individuals who have knowledge related to Apple's infringement of the Authentication Patents including:

- SoC Engineers;[14]
- SoC Design Lead;[15] and
- Senior Manager, Cloud Security Engineering.[16]

These witnesses likely have substantial knowledge regarding Apple's infringement of the Authentication Patents, which disclose a very specific system and system-on-chip ("SoC") architecture as shown in the attached infringement charts. *See* Exs. G-L.

21. Similarly, Apple also currently has multiple job listings in Austin for opportunities related to the SoC directly relevant to the security of the SoC and thus its infringement of the Authentication Patents. For example, Apple is currently seeking a "SoC

---

[11] *Id.* at 8.
[12] *Identity Security LLC*, Dkt. No. 58-1, Ex. Q at 6 (W.D.Tex. Jan. 25, 2022).
[13] *Identity Security LLC*, Dkt. No. 55, at 7–8 (W.D.Tex. Jan. 20, 2022)(Albright, J.)(granting motion to transfer to Austin division).
[14] *See, e.g.*, LinkedIn, *SoC STA Engineer at Apple*, https://www.linkedin.com/in/asritha-chowdary-chunduri/; LinkedIn, *SoC Design Engineer at Apple,* https://www.linkedin.com/in/sandhya-seshadri-5b51763/.
[15] *See, e.g.*, LinkedIn, *SoC Design Lead at Apple Inc.*, https://www.linkedin.com/in/heling-yi-57295a3/.
[16] *See, e.g.*, LinkedIn, *Senior Manager, Cloud Security Engineering at Apple*, https://www.linkedin.com/in/ankitc/.

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

Security Architect, Platform Architecture."[17] The position "will be a key role to help us fulfill our mission with the following core responsibilities: Analysis of Hardware and Software attack vectors[;] Definition of Hardware and Software security related features[;] Architecture of security solutions in HW and SW[;] Development of evaluation plans for both HW and SW[;] Communication with multi-functional teams." Apple is also looking for a SoC Security Engineer, Platform Architecture, who has similar job responsibilities:

Careers at Apple

Work at Apple | Life at Apple | Profile | Sign In | Search

Description

As part of the Platform Architecture organization, the Security Architecture team has a mission to provide rock-solid security foundation to Apple's products. We evaluate security threats, define security features, architect security solutions. We collaborate with the software teams to ensure seamless security systems. We work together with different silicon teams throughout the entire design flow to guarantee state-of-the-art security goes into various in-house and out-sourced silicon chips.

This position will be a key role to help us fulfill our mission with the following core responsibilities:
- Analysis of Hardware and Software attack vectors
- Definition of Hardware and Software security related features
- Architecture of security solutions in HW and SW
- Development of evaluation plans for both HW and SW
- Communication with multi-functional teams

Careers at Apple, *SoC Security Architect, Platform Architecture*, https://jobs.apple.com/en-us/details/200448734/soc-security-engineer-platform-architecture?team=HRDWR (last visited Feb. 27, 2023).

22. Apple currently employs individuals in the Austin metro area who have knowledge related to Apple's infringement of the Fraud Reduction Patents including:

- Software Engineer for iCloud Services and Apple Pay;[18]
- Apple Cash Fraud Protection Specialists;[19] and

[17] Careers at Apple, SoC Security Architect, Platform Architecture, https://jobs.apple.com/en-us/details/200448138/soc-security-architect-platform-architecture?team=HRDWR (last visited Feb. 27, 2023).

[18] *See, e.g.*, LinkedIn, *Software Development Engineer – Apple Pay at Apple*, https://www.linkedin.com/in/anthonylife/.

- Software Quality Engineers, Apple Pay.[20]

23. On information and belief, there are also third-party witnesses in Texas and this District who will have information relevant to Apple's induced infringement of the Authentication Patents. For example, the 1Password platform and password autofill features work in a manner substantially similar to Apple's iCloud Keychain and password autofill features.[21] As alleged below, Apple induces the infringement of 1Password by providing them with APIs, instructions, and other developer tools to use the SoC (specifically the Secure Enclave) and the biometric sensors on each device. Thus, the following 1Password employees likely have knowledge related to Apple's infringing conduct:

- the "Director of Engineering" of 1Password;[22]
- 1Password Software Developer;[23] and
- 1Password Senior iOS Developer.[24]

24. On information and belief, there are also third-party witnesses located in Texas who likely have knowledge relevant to Apple's infringement of the Authentication and Fraud Reduction Patents. Apple's Face ID module, a component of Apple's iOS devices that provides

---

[19] *See, e.g.*, LinkedIn, *Apple Cash Fraud Prevention Team Manager*, https://www.linkedin.com/in/shaun-guhy-61b973184/; *Apple Cash Fraud Analyst*, https://www.linkedin.com/in/chriscasey2/.

[20] *See, e.g.*, Careers at Apple, *Software Quality Engineer, Apple Pay*, https://jobs.apple.com/en-us/details/200336736/software-quality-engineer-apple-pay?team=SFTWR (last visited March 8, 2023).

[21] *See, e.g.*, 1Password, *Secure Enclave Details* (March 2018), https://1password.community/discussion/87886/secure-enclave-details.

[22] LinkedIn, *Director of Engineering at 1Password*, https://www.linkedin.com/in/colehecht/ (last visited Feb. 27, 2023).

[23] LinkedIn, *Software Developer at 1Password*, https://www.linkedin.com/in/kevinfalting/ (last visited Feb. 27, 2023).

[24] LinkedIn, *Senior iOS Developer at 1Password*, https://www.linkedin.com/in/christopheraaron brown/ (last visited Feb. 27, 2023).

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

functionality that infringes the Asserted Patents, is made in Sherman, Texas by the Finisar Corporation. In 2017, Apple invested $390 million in Finisar to develop vertical-cavity surface-emitting laser (VCSEL) technology and related chips for Face ID and other features used in Apple products.[25] In a press release touting its investment in Finisar, Apple highlighted the importance of VCSEL technology to its most successful product lines, noting that "VCSELs power some of Apple's most popular new features, including Face ID, . . . made possible with the iPhone X TrueDepth camera."[26] Apple touted that because of its investment, Finisar would "transform a long-shuttered, 700,000-square-foot manufacturing plant in Sherman, Texas, into the high-tech VCSEL capital of the US."[27]

---

[25] Aishwarya Venugopal, *Apple grants $390 million to Finisar to boost laser chip production*, Reuters, Dec. 13, 2017, https://www.reuters.com/article/uk-apple-finisar-idUKKBN1E71E0.
[26] Apple, *Apple awards Finisar $390 million from its Advanced Manufacturing Fund* (Press Release Dec. 17, 2017), https://www.apple.com/newsroom/2017/12/apple-awards-finisar-390-million-from-its-advanced-manufacturing-fund/.
[27] *Id.*

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

PRESS RELEASE
December 13, 2017

Apple awards Finisar $390 million from its Advanced Manufacturing Fund

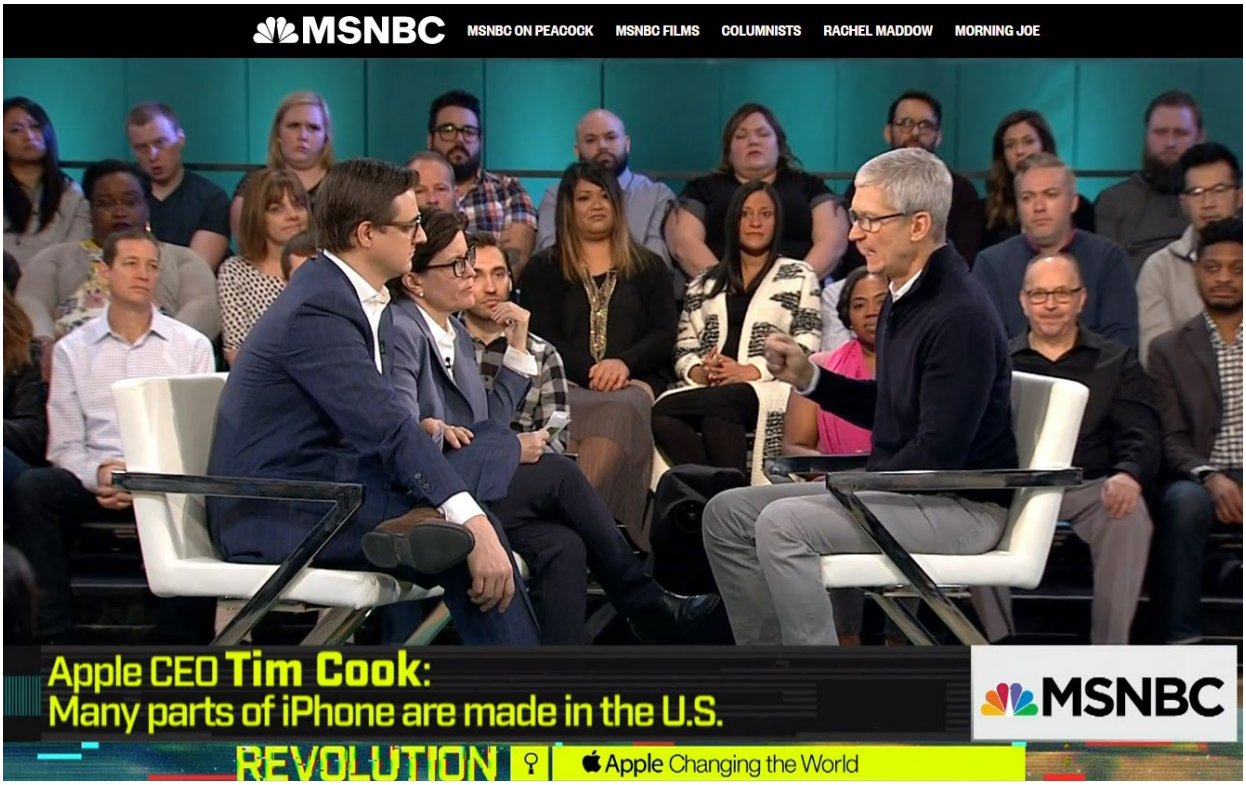
Award Will Create 500 High-Skill Jobs at Sherman, Texas Facility

A Finisar technician examines a wafer during production.

Apple, *Apple awards Finisar $390 million from its Advanced Manufacturing Fund* (Press Release Dec. 17, 2017), https://www.apple.com/newsroom/2017/12/apple-awards-finisar-390-million-from-its-advanced-manufacturing-fund/.

25. Following Apple's investment, in a nationally televised interview on MSNBC in April 2018, Apple CEO Tim Cook confirmed that the "very sophisticated Face ID module on the iPhone X will be made in the United States—in Texas."[28]

[28] *Revolution: Apple Changing the World* (MSNBC television broadcast Apr. 6, 2018) at 1:47, https://www.msnbc.com/msnbc/watch/apple-ceo-tim-cook-on-american-job-opportunity-1204826179812.



Revolution: Apple Changing the World (MSNBC television broadcast Apr. 6, 2018) at 1:47, https://www.msnbc.com/msnbc/watch/apple-ceo-tim-cook-on-american-job-opportunity-1204826179812

26. On information and belief, Finisar continues to make the Face ID module for the latest iPhones and other iOS products in Sherman, Texas, as evidenced by Apple's investment of $410 million in Finisar's parent corporation, II-VI Inc. (now operating as Coherent Corp.), to expand operations at Finisar's Sherman facility and other locations in the United States.[29] Therefore, it is likely that individuals working in Finisar's Sherman facility, or in related positions in Texas, will have information regarding the development and production of the Face ID module that is relevant to Apple's infringement of the Fraud Reduction Patents.[30]

---

[29] David Seeley, *Apple Invests $410M in II-VI Inc., Supporting 700+ Jobs in Sherman and Other U.S. Cities* (May 5, 2021), https://dallasinnovates.com/apple-invests-410m-in-ii-vi-inc-supporting-700-jobs-in-sherman-and-other-u-s-cities/.

[30] *See, e.g.*, LinkedIn, *Lead Product Engineer at Coherent Corp/II-VI Inc./Finisar Corp*, https://www.linkedin.com/in/salman-khalid-16a56116/.

Finisar Considers $3 Billion Semiconductor Expansion Project in Sherman

Finisar's new plant, proposed as an expansion to the tech manufacturers' current 76-acre site in Sherman, would produce wafers for semiconductor chips and create 700 jobs.

Finisar II-VI [File photo: Apple]

David Seeley, *Apple Invests $410M in II-VI Inc., Supporting 700+ Jobs in Sherman and Other U.S. Cities* (May 5, 2021), https://dallasinnovates.com/apple-invests-410m-in-ii-vi-inc-supporting-700-jobs-in-sherman-and-other-u-s-cities/.

27. Finally, venue is also convenient in this District. This is at least true because of this District's close ties to this case—including the technology, relevant witnesses, and sources of proof noted above—and its ability to quickly and efficiently move this case to resolution. Moreover, Apple has previously consented to this Court's jurisdiction and has moved for an intra-district transfer to the Western District of Texas's Austin Division for the convenience of parties and witnesses under 28 U.S.C. § 1404(a) for similar or related technologies. *See SpaceTime3D, Inc. v. Apple Inc.*, No. 6-22-cv-00149, Dkt. No. 34 (W.D. Tex. July 18, 2022);

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

Identity Security LLC v. Apple, Inc., No. 6:21-CV-00460-ADA, Dkt. No. 55, at 7 (W.D. Tex. Jan. 20, 2022).

28. For example, in *Identity Security*, a case related to the Secure Enclave processor, Apple identified multiple employees who work on the relevant technology in Austin—including "the 'lead designer and the lead spec author' of Secure Enclave[.]"[31] In *Identity Security*, Apple moved for transfer to the Austin Division and transfer was granted.

BACKGROUND

29. Carbyne was founded by Dr. Markus Jakobsson with a focus on user authentication and security. Dr. Jakobsson is a preeminent security researcher with interests in applied security, ranging from device security to user interfaces. He is one of the main contributors to the understanding of phishing and crimeware and currently focuses his efforts on social engineering, human aspects of security, and mobile security. Dr. Jakobsson has published a collection of books and over one hundred peer-reviewed conference and journal articles related to user data security.[32]

30. Dr. Jakobsson's passion for user security started while pursuing a degree in computer engineering from the Lund Institute of Technology in Sweden. During his studies, Dr. Jakobsson focused on automated control and robotics; however, Dr. Jakobsson started to notice that the main problem in the field of automated control was related to getting guided missiles to a target. Feeling dismayed about being involved with weapons, Dr. Jakobsson began looking for a path where the main application was not destruction but rather protecting or defending individuals, information, and devices.

---

[31] *Identity Security LLC v. Apple, Inc.*, Case No. 1-22-cv-00058, Dkt. No. 55 at 8, 13 (W.D. Tex. Jan. 20, 2022) (Albright, J.) (granting transfer to Austin)
[32] More information on Dr. Jakobsson can be found at https://www.markus-jakobsson.com/.

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

31. With this in mind, Dr. Jakobsson became interested in computer security, which at its very core is about protecting information and resources. After completing his computer science graduate studies at the University of California San Diego, Dr. Jakobsson realized that most security problems revolved around the divide between a user's security preference and the usability/user experience of a given security feature. For example, a user may prefer to use safe security practices such as complex usernames and passwords; however, the tedious experience of implementing and using a complex password combination may lead users to use less secure, simple passwords or reuse old passwords.

32. One way to address this issue is to use a password manager secured by a user's biometrics. Users are more inclined to use stronger, complex passwords when storing and retrieving the password is as simple as scanning a biometric—such as a fingerprint or face scan—when prompted by a device. However, Dr. Jakobsson knew that despite the advantages of biometrics for storing and securing passwords, if biometric features were not properly deployed, they could be more insecure than traditional passwords.[33] For example, if a user sends biometrics from a device with a biometric reader (like a phone or tablet) to a different device (like a server) for verification, the user is sending their most sensitive data over a network that is out of their control and vulnerable to malicious actors. On the other hand, if a user uses a device with the biometric reader to scan and verify a biometric, the user is storing their most sensitive data—such as their biometrics—in the device's main storage and leaving that data vulnerable to security breaches and malware. Dr. Jakobsson determined that the correct way to deal with this was to create a secure portion of a device where at least some processing of the user's most sensitive data would be done. This solution eliminates the network security issue because that

[33] Unlike a password, a compromised biometric cannot be changed.

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

data is never sent over an unprotected network, and it does not expose the data to breaches and other forms of malware.

33. Dr. Jakobsson also realized that safely storing a user's sensitive data is only one aspect of user security. As the world economy has increasingly moved online, electronic fraud has exploded. Electronic payment fraud is now a multi-billion dollar enterprise, expected to eclipse $48 billion globally in 2023.[34] Electronic fraud is particularly devastating and hard to prevent because the perpetrator does not need physical access to money or a debit card, and there is no transaction that takes place in a physical location. A fraudulent electronic transaction can be completed anywhere, at any time. All that is typically required is access to the Internet and remote access to a victim's online account, smartphone, or computer.

34. In the late 2000's, Dr. Jakobsson recognized the increasing threat posed by electronic fraud and set out to develop better techniques for reducing and deterring fraud in electronic transactions. He started by reading books and journal articles to better understand the psychological factors that will deter a person from committing fraud. Dr. Jakobsson first considered the motivations underlying "friendly fraud"—fraud committed by a friend or family member. He learned that particularly with friendly fraud, feelings of guilt will often deter a person from committing fraud. One way to increase the potential fraudster's feelings of guilt is to humanize the transaction by associating the transaction with an actual person.

35. But increasing feelings of guilt alone is often not enough to deter fraud, particularly if the perpetrator has no connection to a person associated with an electronic transaction. In his research, Dr. Jakobsson also learned that another reason, perhaps the most

---

[34] *Juniper Research: eCommerce Losses to Online Payment Fraud to Exceed $48 Billion Globally in 2023, as Fraud Incursions Evolve,* Yahoo! (Oct. 12, 2022), https://www.yahoo.com/now/juniper-research-ecommerce-losses-online-060000415.html.

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

compelling reason, why an otherwise honest person might be tempted to commit fraud is that the risk of being caught is low. With this in mind, Dr. Jakobsson determined that a key factor in preventing or reducing fraud is to both increase the likelihood that the fraudulent transaction will be detected and to cause the fraudster to believe that his or her fraudulent actions will be detected.

36. Dr. Jakobsson realized that improving the ability to detect fraud in electronic transactions would require a technological solution. He determined that possible solutions could include collecting a user's location data or biometric information (e.g., requiring a user to take a photograph of himself) to complete an electronic transaction. But Dr. Jakobsson realized that relying on a single photograph of the user or other basic biometric methods to authenticate an electronic transaction would be insufficient. A fraudster could defeat such countermeasures—for example, by using a two-dimensional photograph of a legitimate user. Dr. Jakobsson determined that a better fraud detection measure would be collecting a user's biometric information and analyzing it in a way that verifies the user is "alive" before authorizing an electronic transaction. The "aliveness" verification would be more difficult for the fraudster to defeat, thus increasing the likelihood that a potential fraudulent transaction would be detected and prevented. And so Dr. Jakobsson's idea for the Fraud Reduction Patents was born.

THE CARBYNE PATENTS

A. The Authentication Patents[35]

37. On February 23, 2021, the U.S. Patent and Trademark Office duly and legally issued U.S. Patent No. 10,929,512 ("the '512 Patent"), entitled "Authentication Translation," to inventor Bjorn Markus Jakobsson. Carbyne owns all rights to the '512 Patent necessary to bring

[35] The Authentication Patents share a specification. Unless otherwise noted, the citations are to the '512 Patent's specification.

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

this action. A true and correct copy of the ’512 Patent is attached hereto as Exhibit A and incorporated herein by reference.

38. On October 18, 2022, the U.S. Patent and Trademark Office duly and legally issued U.S. Patent No. 11,475,105 (“the ’105 Patent”), entitled “Authentication Translation,” to inventor Bjorn Markus Jakobsson. Carbyne owns all rights to the ’105 Patent necessary to bring this action. A true and correct copy of the ’105 Patent is attached hereto as Exhibit B and incorporated herein by reference.

39. On November 29, 2022, the U.S. Patent and Trademark Office duly and legally issued U.S. Patent No. 11,514,138 (“the ’138 Patent”), entitled “Authentication Translation,” to inventor Bjorn Markus Jakobsson. Carbyne owns all rights to the ’138 Patent necessary to bring this action. A true and correct copy of the ’138 Patent is attached hereto as Exhibit C and incorporated herein by reference.

40. The ’512 Patent concerns systems and methods for authentication translation. As the Patent explains, previous authentication techniques made “[p]roviding credentials to a service, whether via a mobile or other device . . . a tedious experience for a user.” Ex. A (’512 Patent) at 1:35-37. Because the experience was so tedious, users would “often engage in practices such as password re-use, and/or the selection of poor-quality passwords, which render their credentials less secure against attacks.” *Id*. at 1:38-40. Thus, “improvements in authentication techniques [were] desirable.” *Id*. at 1:40-42.

41. The ’512 Patent addresses these shortcomings by disclosing novel authentication systems and methods. The ’512 Patent discloses methods and systems where “users need not type such usernames and passwords into their devices whenever required by a service. Instead, users can authenticate themselves to an ‘authentication translator’ via an appropriate technique,

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

and the authentication translator will provide the appropriate credentials to the implicated service on the user's behalf." *Id*. at 2:63-3:1. By doing this, the system promotes better user security practices by making it easier for a user to use complex passwords.

42. As the '512 patent discloses, the process begins "when a request to access a resource is received, as is an authentication input." *Id.* at 6:20-21. For example, suppose "[the user] wishes to sign into social networking website." *Id*. at 6:22-23. "[The user] directs [their] web browser . . . to the social networking website." *Id*. at 6:23-25. The "Authentication translator module **132** recognizes, from the context of [the user's] actions (e.g., that [the user] is attempting to access site **120** with [their] browser) that [the user] would like to access a particular resource." Ex. A ('512 Patent) at 6:25-28 (emphasis in original). The authentication translator module may then prompt "[the user] (e.g., by a popup message or via a sound) to provide biometric information (e.g., to use the integrated fingerprint reader on [the user's device])." *Id.* at 6:28-31.

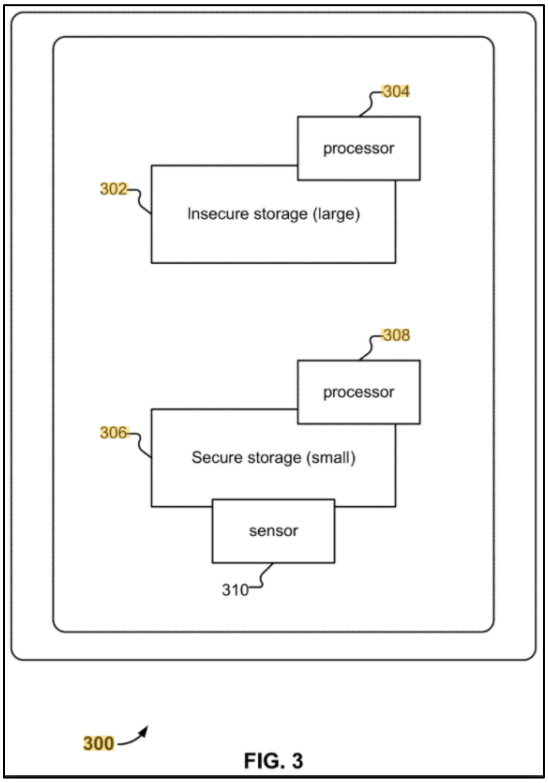
43. Once a biometric has been supplied by the user, the supplied biometric data is compared "to the templates stored on [the user's device]." *Id*. at 6:39-40. "If a suitable match is found . . . the username and password for the website, as stored in a vault, such as vault **220**, are retrieved from the vault" and provided to the resource. *Id*. at 6:40-46 (emphasis in original). In the '512 Patent specification, biometrics include but are not limited to fingerprints, "facial recognition, voiceprints, or retina scan technology." *Id*. at 3:28-29, 3:18-19.

44. To keep the user's biometrics secure, the '512 Patent discloses a device with "a large and insecure storage **302** attached to a fast processor **304**, and a smaller but secure storage **306** attached to a dedicated processor **308** and a sensor **310** (e.g., a camera or a fingerprint reader)." *Id*. at 3:67-4:4 (emphasis in original); *see also id.* at Fig. 3 (reproduced below). The "Users (and applications) can read from and write to the insecure storage area." *Id*. at 4:4-5. Data

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

such as authentication information and biometrics can be stored in the secure storage. *Id*. at 3:63-65. "However, users cannot access the secure storage area, and the fast processor can only communicate with the dedicated processor/sensor via a restricted API." *Id*. at 4:5-8.

45. Figure 3 of the '512 Patent, which depicts a device with large and insecure storage attached to a fast processor, and a smaller but secure storage attached to a dedicated processor and a sensor in accordance with an embodiment of the inventions, is reproduced below.



Ex. A ('512 Patent) at Fig. 3.

46. Further enhancing the user authentication experience and promoting better security practices across multiple devices, the '512 Patent also discloses uploading a secure back up of the records stored in the secure storage to a cloud storage service. *Id*. at 7:55-8:8. "The cloud storage service **140** is configured to accept backups from multiple devices associated with

a single account, and synchronize the updates so that all devices get automatically refreshed." *Id*. at 7:56-59 (emphasis in original). This allows a user to access and synchronize authentication information across multiple devices, *id*. at 7:59-62, further reducing the tedious experience of using complex passwords.

47. Further enhancing the user authentication experience and promoting better security practices across multiple devices, the '105 Patent also discloses a "same brand" backup where, for example, "vaults can only be backed up to computational devices of the same brand." Ex. B ('105 Patent) at 19:28-32. This is important because having control within the same brand enables stronger security. For example, in a scenario where the solution relies on key distribution or access control (say to the storage), doing it in-brand enables additional assurances and controls.

48. Further, enhancing the user authentication experience and promoting better security practices across multiple devices, the '138 Patent also discloses specifically using a cryptographic key as the credential. This is important because as the Patent explains, a "cryptographic key [can be used] for service providers supporting stronger authentication methods." Ex. C ('138 Patent) at 3:61-64. Further, the '138 discusses and claims facilitating the wiping of the key.

49. These advances are also reflected in the claims of each of the Authentication Patents. *See, e.g.*, Exs. A-C at claim 1. Accordingly, the claims of the Authentication Patents recite one or more inventive concepts rooted in computerized technology and overcome technical problems in that field. A person of ordinary skill in the art reading the Authentication Patents and their claims would understand that the Patents' disclosure and claims are drawn to solving specific, technical problems arising in authentication systems/methods and provide for

advancements in the field that were not routine, well-understood or conventional. Accordingly, the claims of the Authentication Patents recite a combination of elements sufficient to ensure that the claims in practice amount to significantly more than a patent claiming an abstract concept. A person of ordinary skill in the art would understand that the ordered combination of claim elements is inventive. Further, the claimed improvements over prior art authentication systems are concrete and improve the capabilities of existing authentication translation systems/methods.

50. A person of ordinary skill in the art reviewing the specification of the Authentication Patents would understand that the inventor had possession of the claimed subject matter and would know how to practice the claimed invention without undue experimentation.

B. The Fraud Reduction Patents[36]

51. On May 15, 2018, the U.S. Patent and Trademark Office duly and legally issued U.S. Patent No. 9,972,010 ("the '010 Patent"), entitled "Method, Medium, and System for Reducing Fraud," to inventor Bjorn Markus Jakobsson. Carbyne owns all rights to the '010 Patent necessary to bring this action. A true and correct copy of the '010 Patent is attached hereto as Exhibit D and incorporated herein by reference.

52. On July 14, 2020, the U.S. Patent and Trademark Office duly and legally issued U.S. Patent No. 10,713,656 ("the '656 Patent"), entitled "Method, Medium, and System for Reducing Fraud," to inventor Bjorn Markus Jakobsson. Carbyne owns all rights to the '656 Patent necessary to bring this action. A true and correct copy of the '656 Patent is attached hereto as Exhibit E and incorporated herein by reference.

53. On December 13, 2022, the U.S. Patent and Trademark Office duly and legally issued U.S. Patent No. 11,526,886 ("the '886 Patent"), entitled "Method, Medium, and System

[36] The Fraud Reduction Patents share a common specification. Unless otherwise noted, all citations are to the '010 Patent.

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

for Reducing Fraud," to inventor Bjorn Markus Jakobsson. Carbyne owns all rights to the '886 Patent necessary to bring this action. A true and correct copy of the '886 Patent is attached hereto as Exhibit F and incorporated herein by reference.

54. The Fraud Reduction Patents generally relate to systems and methods for preventing or reducing fraud in electronic transactions. As the Patents explain, fraudulent transactions "are an ongoing problem." Ex. D ('010 Patent) at 1:19. One reason that a person might engage in a fraudulent transaction is that "the risk of being caught is low." *Id.* at 7:32-33. By its nature, electronic fraud "can be particularly devastating because the perpetrator does not need physical access to a victim's credit card (or other resource) to perform the fraud." *Id.* 1:24-27. Because no physical interaction with the victim is required, electronic fraud can be perpetrated remotely from anywhere in the world by accessing an electronic account belonging to the victim, making it more difficult to detect the fraud and less likely that the perpetrator will be identified.

55. The Fraud Reduction Patents address the "ongoing problem" of electronic fraud by providing fraud detection technology that "increase[s] the likelihood (either real or perceived by the fraudster) that the fraudulent act will be detected." *Id.* at 4:46-48. At a high level, the claimed fraud detection process proceeds as follows. The process begins when a person (the "user") initiates an electronic transaction. The user is presented with an interface containing a "transaction icon." *See* Exs. D-F at claim 1. The user interacts with the transaction icon in the interface. *See id*. The user's biometric information is then captured and fraud detection analysis is performed to determine that the user is alive, based at least in part on the biometric information collected from the user. *See id.* The electronic transaction is then completed based at

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

least in part on both the user interaction with the transaction icon in the interface and the fraud detection analysis. *See id.*

56. While the preceding paragraph describes the general fraud detection and reduction process, the Fraud Reduction Patents vary to some degree in how they complete the fraud detection analysis.

57. The fraud detection analysis for the ’010 Patent most closely aligns with the process just described. It requires capturing “contextual information associated with the electronic transaction, the captured information comprising captured biometric information associated with a user” and “determining, based in part on the captured biometric information, that the user is alive.” Ex. D (’010 Patent) at claim 1 (14:5-9, 12-14).

58. For the ’656 Patent, following the user’s interaction with the transaction icon, the user’s biometric information is captured, along with “location data associated with the user.” Ex. E at 14:12-16. The fraud detection analysis then comprises “performing a comparison based at least in part on the stored biometric information and the captured biometric information; and determining, based at least in part on the captured biometric information, that the user is alive.” Ex. E (’656 Patent) at claim 1 (14:21-25).

59. For the ’886 Patent, following the user’s interaction with the transaction icon, the claimed fraud detection measures first require the capture of “contextual information comprising location data usable to determine a physical location associated with the user” and “a set of biometric information, wherein capturing the set of biometric information comprises capturing, using a camera, a set of images.” Ex. F (’886 Patent) at claim 1 (14:8-15). Fraud detection analysis is then performed to determine whether to allow an electronic transaction to proceed based at least in part on “the physical location associated with the user determined using the

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

captured location data; and an analysis of the set of captured biometric information comprising a determination of whether the user is alive based at least in part on an analysis of the set of images captured using the camera." *Id.* at claim 1 (14:20-25).

60. As the preceding paragraphs demonstrate, the claims and specification of the Fraud Reduction Patents recite specific improvements for techniques for detecting and reducing fraud in electronic transactions. Specifically, the Fraud Reduction Patents provide a technological solution for the problem of detecting electronic fraud by capturing biometric information associated with a user initiating an electronic transaction and analyzing that information to determine that the user is alive. *See* Ex. D ('010 Patent) at 8:54-67 and Exs. D-F at claim 1. The Patents disclose several techniques for determining a user's aliveness. For example, "multiple photographs" of the user can be taken in "rapid succession" prior to completing the electronic transaction to "make sure that [a] fraudster isn't using [a] camera [] to photograph a printed picture of the legitimate user." Ex. D ('010 Patent) at 8:55-60; *see also* Ex. F ('886 Patent) at claim 1. The use of multiple photographs to determine a user's "aliveness" is a direct technological improvement over other fraud reduction measures that take a single photograph of the user and can be fooled by a two-dimensional image. Other examples of technological means for determining the user's aliveness that the Patents disclose include requiring a user to turn on a device's GPS prior to a transaction taking place, or requiring the user to provide a voice sample to ensure the user is indeed a human being. Ex. D ('010 Patent) at 8:63-67. Finally, by requiring collection of location data for the user initiating the electronic transaction, the Patents provide another technological measure for detecting potential fraud and identifying the perpetrator. *See, e.g.* Ex. E ('656 Patent) and Ex. F ('886 Patent) at claim 1.

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

61. In sum, the claims of the Fraud Reduction Patents recite one or more inventive concepts rooted in computerized technology for detecting and reducing fraud in electronic transactions and, as explained above, overcome specific technical problems in this field. A person of ordinary skill in the art reading the Fraud Reduction Patents and their claims would understand that the Patents' disclosures and claims are drawn to solving specific, technical problems arising in systems and methods for reducing fraud in electronic transactions and provide for advancements in the field that were not routine, well-understood, or conventional. Accordingly, the claims of the Fraud Reduction Patents recite a combination of elements sufficient to ensure that the claims in practice amount to significantly more than a patent claiming an abstract concept. A person of ordinary skill in the art would understand that the ordered combination of claim elements is inventive. Further, the claimed improvements over prior art systems and methods for reducing fraud in electronic transactions are concrete and improve the capabilities of existing systems and methods for reducing electronic fraud.

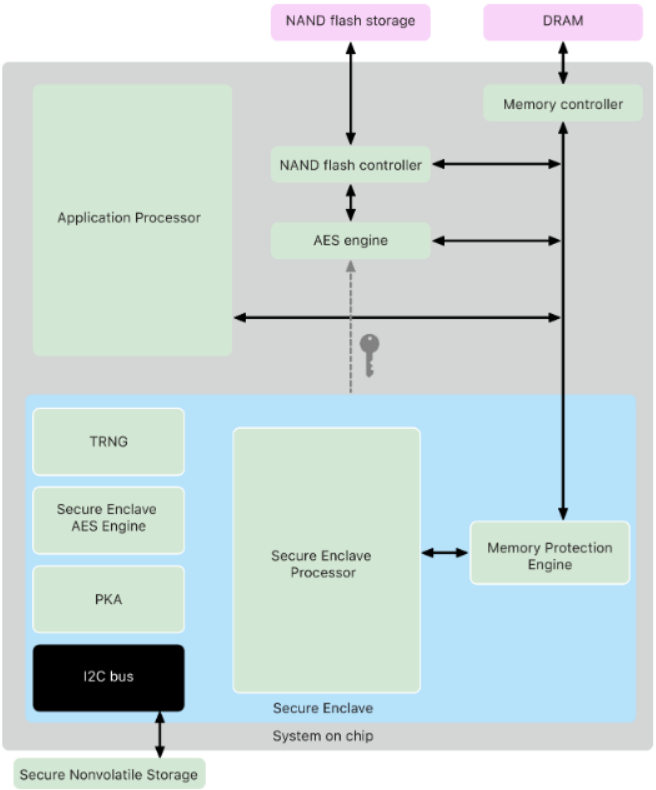
62. A person of ordinary skill in the art reviewing the specification of the Fraud Reduction Patents would understand that the inventor had possession of the claimed subject matter and would know how to practice the claimed invention without undue experimentation.

APPLE'S USE OF CARBYNE'S PATENTED TECHNOLOGY

63. As set forth below and in the attached exemplary infringement charts, seeking to differentiate itself from its competitors, Apple turned to Carbyne's patented technology to improve user security in ***all*** of its new M-Series Macs and A-Series iOS devices by enabling the "Secure Enclave" for authentication. "The Secure Enclave is a dedicated secure subsystem

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

integrated into Apple systems on chip (SoCs)" such as the A- and M-Series chips.[37] "The Secure Enclave is isolated from the main processor to provide an extra layer of security and is designed to keep sensitive user data secure even when the Application Processor kernel becomes compromised."[38] Further, "[a]lthough the Secure Enclave doesn't include storage, it has a mechanism to store information securely on attached storage separate from the NAND flash storage that's used by the Application Processor and operating system."[39]



[37] Apple, *Apple Platform Security: May 2022* at 9, https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.
[38] *Id.*
[39] *Id.*

The Secure Enclave is a hardware feature of most versions of iPhone, iPad, Mac, Apple TV, Apple Watch, and HomePod—namely:

- iPhone 5s or later
- iPad Air or later
- MacBook Pro computers with Touch Bar (2016 and 2017) that contain the Apple T1 Chip
- Intel-based Mac computers that contain the Apple T2 Security Chip
- Mac computers with Apple silicon
- Apple TV HD or later
- Apple Watch Series 1 or later
- HomePod and HomePod mini

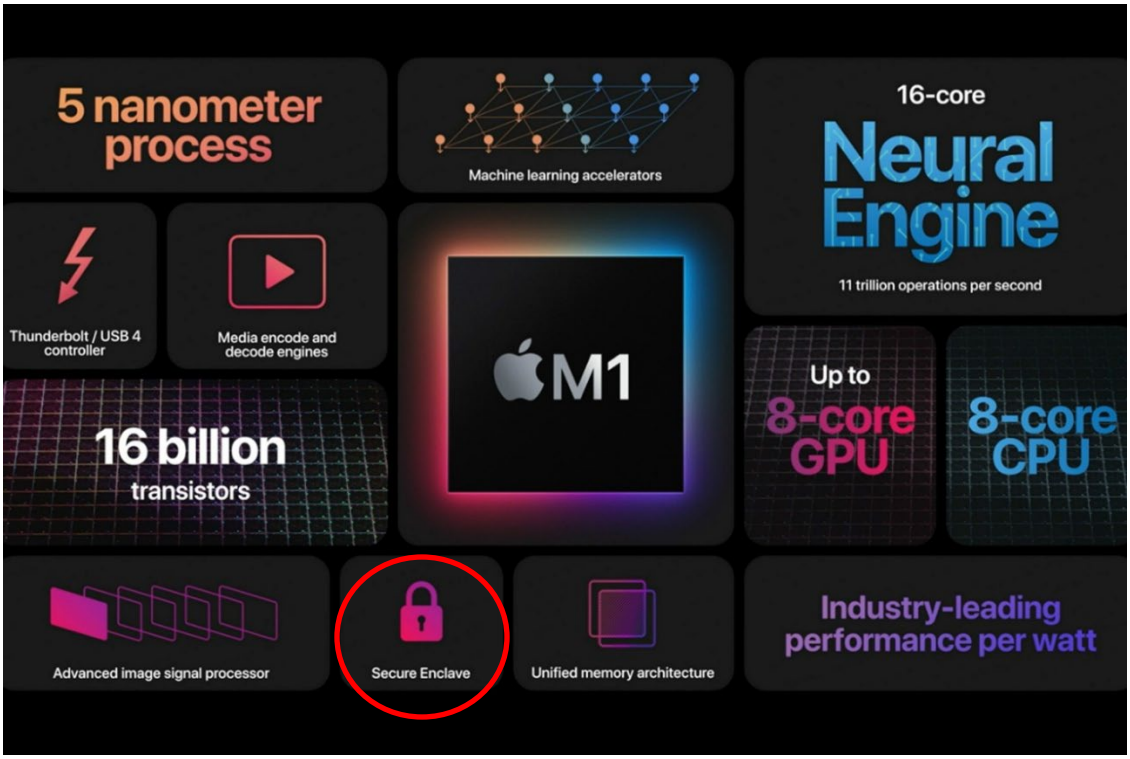
Secure Enclave Processor

The Secure Enclave Processor provides the main computing power for the Secure Enclave. To provide the strongest isolation, the Secure Enclave Processor is dedicated solely for Secure Enclave use. This helps prevent side-channel attacks that depend on malicious software sharing the same execution core as the target software under attack.

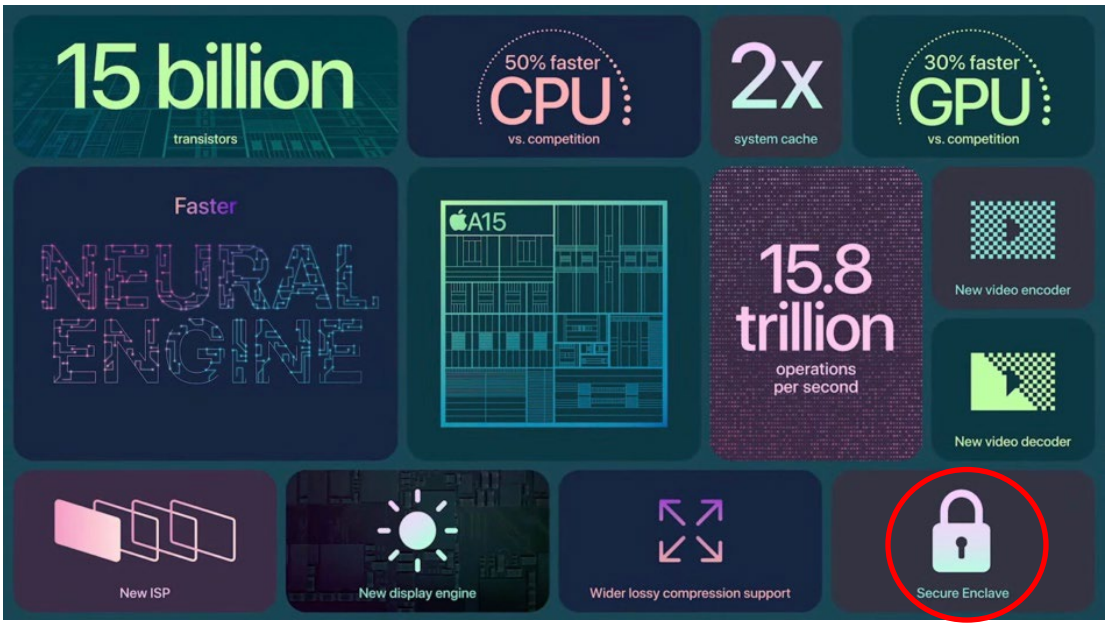
The Secure Enclave Processor runs an Apple-customized version of the L4 microkernel. It's designed to operate efficiently at a lower clock speed that helps to protect it against clock and power attacks. The Secure Enclave Processor, starting with the A11 and S4, includes a memory-protected engine and encrypted memory with anti-replay capabilities, secure boot, a dedicated random number generator, and its own AES engine.

Apple, *Apple Platform Security: May 2022* at 9-10, https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.

64. Apple touts the Secure Enclave as a selling point on all of its devices. For example, during consumer product announcements for devices, Apple routinely includes the Secure Enclave on the product overview slide.



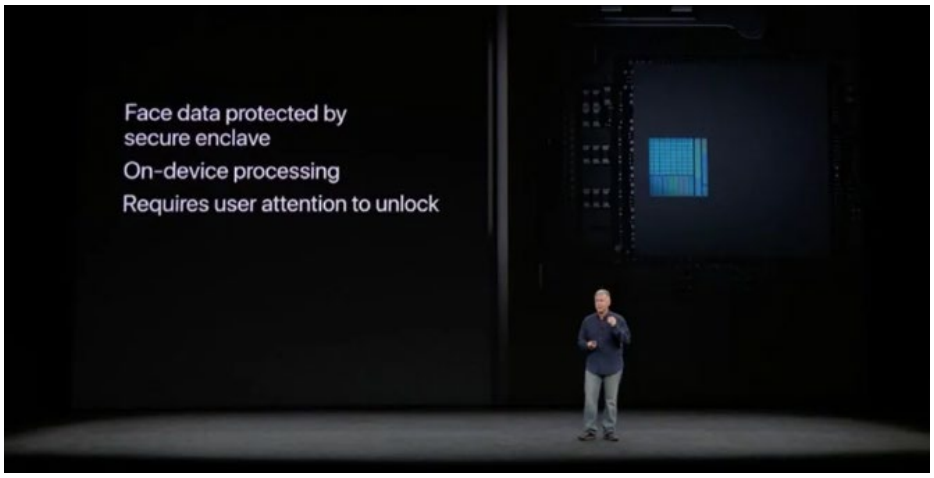
Macworld, *The M1 chip and beyond: Everything you need to know about Apple's homegrown Mac chips* (Aug. 5, 2022), https://www.macworld.com/article/234860/apple-silicon-m1-system-on-chip-macbook-air-macbook-pro-mac-mini-imac-m1x-specs-features-intel-apps-rosetta-2.html



Apple Event – September 14, 2021, YouTube, https://www.youtube.com/watch?v=EvGOlAkLSLw.

65. Apple also publishes extensive security guides and consumer-oriented articles, such as the Apple Platform Security guide, that explain how the Secure Enclave protects user data and how to use the Secure Enclave in combination with the Password Autofill and other biometric features.[40]

66. Further, Apple touts its biometric scanners such as Face ID and Touch ID as being protected by the Secure Enclave.



Ben Lovejoy, *Apple's Secure Enclave set a security precedent for Android smartphones*, 9to5Mac (Feb. 12, 2020), https://9to5mac.com/2020/02/12/apples-secure-enclave/.

[40] *See* Apple, *Apple Platform Security: May 2022*, https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.

Apple explains Touch ID in depth with latest iOS security document

Zac Hall | Feb 26 2014 - 2:17 pm PT 11 Comments

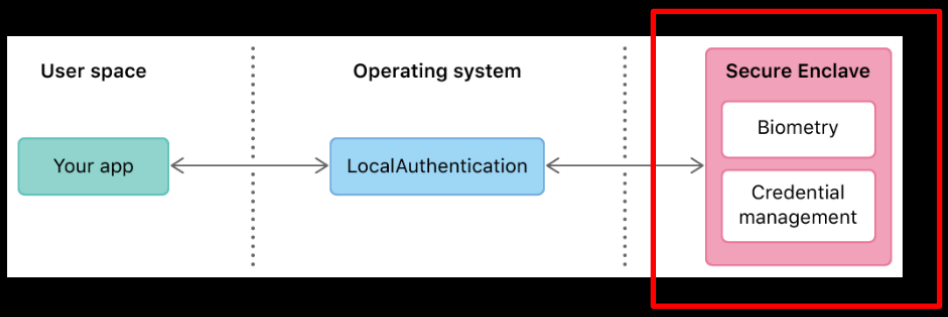
In the latest release of its iOS Security document spotted by *TechCrunch*, Apple offers a number of details about the function and processes of the Touch ID fingerprint recognition system offered on its iPhone 5s. The document describes the Secure Enclave, "a coprocessor fabricated in the Apple A7 chip," which manages safely matching active fingerprints read by Touch ID against registered fingerprints saved by the user. While much of how Touch ID behaves was revealed last fall when the iPhone 5s was introduced and through experience, the white page does list more specifics than have previously been made available...

Zac Hall, *Apple explains Touch ID in depth with latest iOS security document*, 9to5Mac (Feb 26 2014), https://9to5mac.com/2014/02/26/apple-explains-touch-id-in-depth-with-latest-ios-security-document/.

67. Finally, Apple discusses the advantages of the patented technology when it informs its developers how to access and use the Secure Enclave, Face ID and Touch ID, and the authentication framework in the developers' applications and services.

Overview

Many users rely on biometric authentication like Face ID or Touch ID to enable secure, effortless access to their devices. As a fallback option, and for devices without biometry, a passcode or password serves a similar purpose. Use the LocalAuthentication framework to leverage these mechanisms in your app and extend authentication procedures your app already implements.



To maximize security, your app never gains access to any of the underlying authentication data. You can't access any fingerprint images, for example. The Secure Enclave, a hardware-based security processor isolated from the rest of the system, manages this data out of reach even of the operating system. Instead, you specify a particular policy and provide messaging that tells the user why you want them to authenticate. The framework then coordinates with the Secure Enclave to carry out the operation. Afterward, you receive only a Boolean result indicating authentication success or failure.

Apple, *Local Authentication: Authenticate users biometrically or with a passphrase they already know*, https://developer.apple.com/documentation/localauthentication/ (last visited Feb. 27, 2023).

68. Apple has also turned to Carbyne's patented technology to reduce fraud across its Apple Cash payment platform. The Apple Cash platform allows two individuals to complete a user-to-user cash transfer by using Apple's iMessage or Apple Wallet applications on either an iPhone or iPad.[41] To perform an Apple Cash transaction, both the sender and recipient must have an iCloud account and Apple ID that are linked to a debit card in the Apple Wallet application.

[41] Apple Cash and Apple Wallet are components of the overarching Apple Pay platform. *See* Apple, *Apple Pay*, https://www.apple.com/apple-pay/ (last visited Mar. 9, 2023).

The sender initiates a transaction by either selecting the Apple Cash card in the sender's Apple Wallet and identifying the recipient or initiating a conversation with the intended recipient in the iMessage application and clicking the Apple Cash icon in the iMessage interface. The sender then selects the amount of cash to be transferred, and sends a payment request. The sender is then prompted to confirm the transaction, which activates Apple's Face ID feature. *See* Exs. M-O.

69. Apple's Face ID feature in turn relies on Carbyne's patented technology to complete the Apple Cash transaction. The Face ID feature uses a TrueDepth camera on the sender's device to take multiple photos of the sender's face. Upon information and belief, the Face ID feature then performs an analysis using these photos to verify, among other things, that the sender is alive and not a two-dimensional photograph. Once the Face ID scan is successfully completed, the Apple Cash transfer is processed. *See* Exs. M-O.

70. The Apple Cash platform also implements Carbyne's patented fraud reduction technology by detecting the sender's physical location before a transfer can be successfully processed. Apple Cash transfers can only be completed if the sender is located in the United States. So in order to complete a transaction, the Apple Cash platform relies on location data captured by the sender's device to determine that the sender is located in the United States.

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

If you can't send or receive money with Apple Cash

If you try to use Apple Cash to send or receive money and need help, try these steps.

First, check the Apple System Status page to make sure there are no outages or scheduled maintenances currently affecting Apple Cash.

What you need to send or receive money

To send and receive money using Apple Cash, you must be a resident of the United States and your device must be in the United States.[1] If you're under 18 years old, your family organizer must set up Apple Cash for you as part of Apple Cash Family. Then, you can send and receive money in Messages or Wallet.

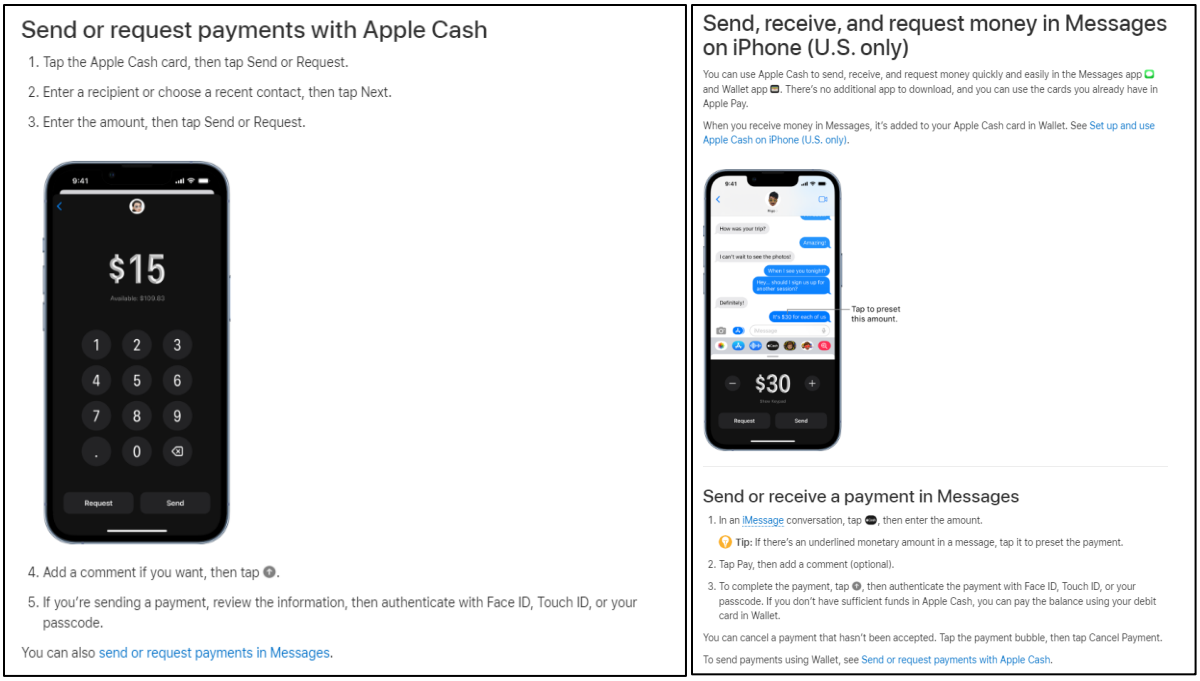
To make sure that you have everything you need, follow these steps:

1. Check for iOS or watchOS updates.
2. Make sure that your device is eligible.
3. Make sure that you have a Wi-Fi or cellular connection.
4. Sign in to iCloud and iMessage with the same Apple ID on any device that you want to use to send or receive money:
   - iCloud: Tap Settings > [your name].
   - iMessage: Tap Settings > Messages > Send & Receive.

Apple, *Apple Support: If you can't send or receive money with Apple Cash*, https://support.apple.com/en-us/HT207933 (last visited Feb. 27, 2023).

71. Apple has multiple webpages explaining to users how to use the infringing technology when they make an Apple Cash transaction.[42] For example, as shown below, Apple instructs users how to complete a payment through iMessage or the wallet application.

[42] *See, e.g.*, Apple, *Apple Cash*, https://www.apple.com/apple-cash/ (last visited Mar. 6, 2023).



Send or request payments with Apple Cash

1. Tap the Apple Cash card, then tap Send or Request.
2. Enter a recipient or choose a recent contact, then tap Next.
3. Enter the amount, then tap Send or Request.

4. Add a comment if you want, then tap.
5. If you're sending a payment, review the information, then authenticate with Face ID, Touch ID, or your passcode.

You can also send or request payments in Messages.

Send, receive, and request money in Messages on iPhone (U.S. only)

You can use Apple Cash to send, receive, and request money quickly and easily in the Messages app and Wallet app. There's no additional app to download, and you can use the cards you already have in Apple Pay.

When you receive money in Messages, it's added to your Apple Cash card in Wallet. See Set up and use Apple Cash on iPhone (U.S. only).

Send or receive a payment in Messages

1. In an iMessage conversation, tap, then enter the amount.

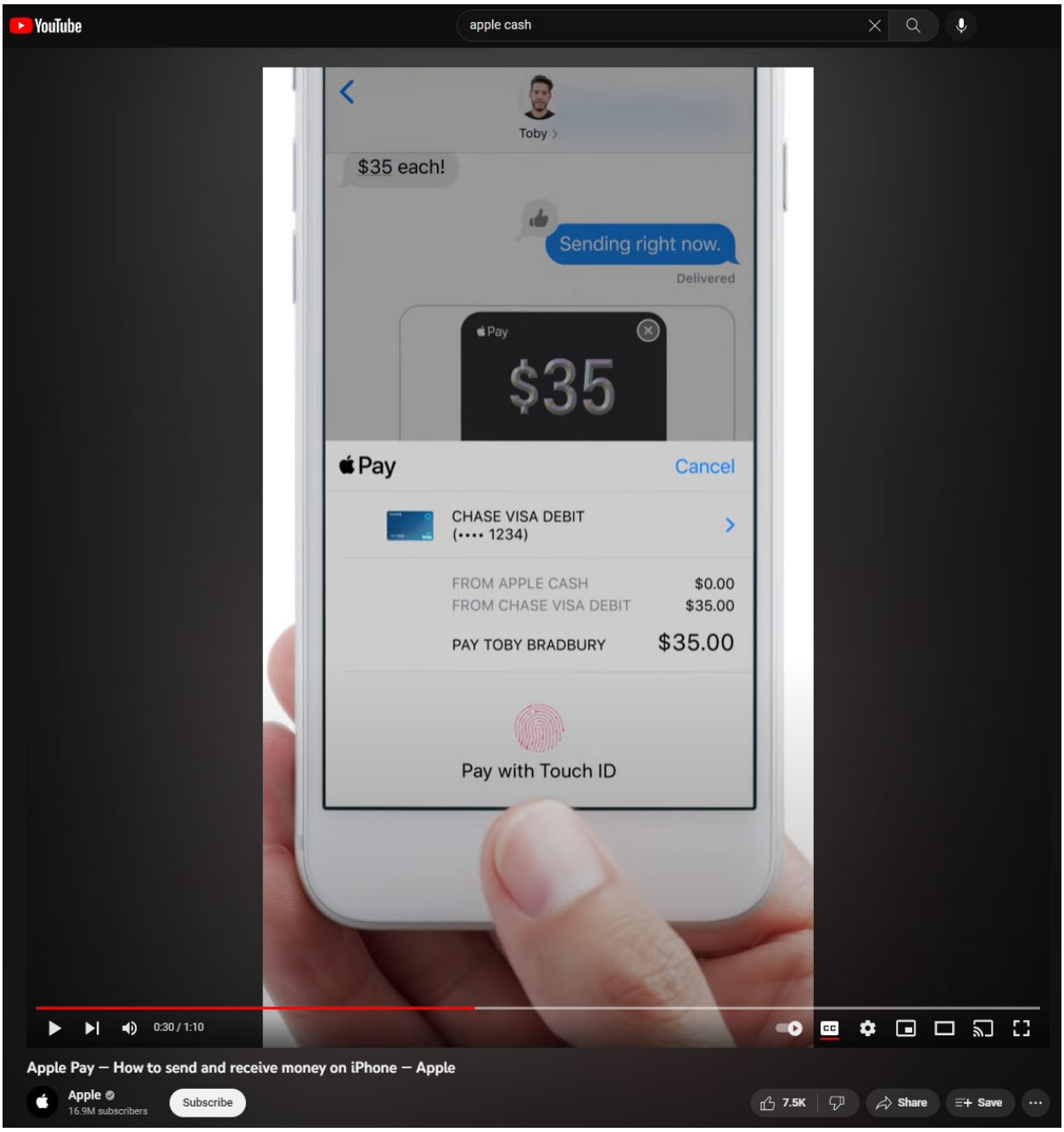
   Tip: If there's an underlined monetary amount in a message, tap it to preset the payment.
2. Tap Pay, then add a comment (optional).
3. To complete the payment, tap, then authenticate the payment with Face ID, Touch ID, or your passcode. If you don't have sufficient funds in Apple Cash, you can pay the balance using your debit card in Wallet.

You can cancel a payment that hasn't been accepted. Tap the payment bubble, then tap Cancel Payment.

To send payments using Wallet, see Send or request payments with Apple Cash.

Apple, *Apple Support: Set up and use Apple Cash on iPhone (U.S. only)*, https://support.apple.com/guide/iphone/use-apple-cash-iph385cf0980/ios (last visited Feb. 27, 2023); Apple, *iPhone User Guide*, https://support.apple.com/guide/iphone/send-receive-request-money-apple-cash-iph6d80edff1/16.0/ios/16.0#iphdf3cf2052 (last visited Feb. 27, 2023).

72. Apple also has consumer oriented videos instructing users how to use the infringing technology.



Apple Pay – How to send and receive money on iPhone – Apple, YouTube (Dec. 6, 2017) https://www.youtube.com/watch?v=znyYodxNdd0.

73. The attached infringement charts explain in greater detail all the ways in which the accused Apple products use Carbyne's patented technology. *See* Exs. M-O.

CLAIMS FOR PATENT INFRINGEMENT[43]

74. The Authentication Patents are infringed by at least all A-Series iOS/iPadOS devices with Touch ID or Face ID and by all M-Series Macs with a built-in Touch ID sensor or paired with an Apple Magic Keyboard with Touch ID.

75. The Fraud Reduction Patents are infringed by at least all of the iOS or iPadOS devices with Face ID.

COUNT I: PATENT INFRINGEMENT OF THE ’512 PATENT

76. Carbyne incorporates by reference the preceding paragraphs as though fully set forth herein.

77. Apple has directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least claims 1-4, 10-14, and 20-21 of the ’512 Patent by making, testing, using, selling, and/or offering for sale its A-Series iOS devices and M-Series Macs in the United States, in violation of 35 U.S.C. § 271(a). *See* Exs. G-H.

78. Apple’s A-Series iOS devices and M-Series Macs, meet each and every element of at least claims 1-4, 10-14, and 20-21 of the ’512 Patent, either literally or equivalently.

79. Apple has had actual and/or constructive knowledge of the existence of the ’512 Patent since no later than the filing of this Original Complaint.

80. With knowledge of the ’512 Patent, at least as of the Complaint, Apple has indirectly infringed one or more claims thereof under 35 U.S.C. § 271(b) through the active inducement of direct infringement by intending to encourage, and in fact encouraging others to install software updates on the A-Series iOS devices and M-Series Macs sold and used within the

---

[43] The following claims and accused products are only exemplary and based on public information. Apple’s infringement is far reaching and Carbyne will identify all of the infringing claims and products when it is required to by the Court’s scheduling order.

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

United States in an infringing manner that practiced the inventions claimed by the ’512 Patent, including at least claims 1-4, 10-14, and 20-21. Apple has actively induced such direct infringement through its communications with customers, thereby providing, *inter alia*, functionality, instructions, and other assistance that have served to facilitate, promote, and cause users of Apple A-Series iOS devices and M-Series Macs, and potentially others yet unknown, to directly infringe at least claims 1-4, 10-14, and 20-21 of the ’512 Patent, as described in Exs. G and H. Upon information and belief, Apple has performed the acts that constitute inducement of infringement with the knowledge or willful blindness that the resulting acts induced thereby would constitute direct infringement by users of Apple A-Series iOS devices and M-Series Macs, and/or potentially by others as yet unknown.

81. As a direct and proximate consequence of Apple’s infringement of the ’512 Patent, Carbyne has suffered damages in an amount not yet determined for which Carbyne is entitled to relief.

COUNT II: PATENT INFRINGEMENT OF THE ’105 PATENT

82. Carbyne incorporates by reference the preceding paragraphs as though fully set forth herein.

83. Apple has directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least claims 1, 9, 18, 28, 35 of the ’105 Patent by making, testing, using, selling, and/or offering for sale its A-Series iOS devices and M-Series Macs in the United States, in violation of 35 U.S.C. § 271(a). *See* Exs. I and J.

84. Apple’s A-Series iOS devices and M-Series Macs, meet each and every element of at least claims 1, 9, 18, 28, 35 of the ’105 Patent, either literally or equivalently.

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

85. Apple has had actual and/or constructive knowledge of the existence of the ’105 Patent since no later than the filing of this Original Complaint.

86. With knowledge of the ’105 Patent, at least as of the Complaint, Apple has indirectly infringed one or more claims thereof under 35 U.S.C. § 271(b) through the active inducement of direct infringement by intending to encourage, and in fact encouraging others to install software updates on the A-Series iOS devices and M-Series Macs sold and used within the United States in an infringing manner that practiced the inventions claimed by the ’105 Patent, including at least claims 1, 9, 18, 28, 35. Apple has actively induced such direct infringement through its communications with customers, thereby providing, *inter alia*, functionality, instructions, and other assistance that have served to facilitate, promote, and cause users of Apple A-Series iOS devices and M-Series Macs, and potentially others yet unknown, to directly infringe at least claims 1, 9, 18, 28, 35 of the ’105 Patent, as described in Exs. I and J. Upon information and belief, Apple has performed the acts that constitute inducement of infringement with the knowledge or willful blindness that the resulting acts induced thereby would constitute direct infringement by users of Apple A-Series iOS devices and M-Series Macs, and/or potentially by others as yet unknown.

87. As a direct and proximate consequence of Apple’s infringement of the ’105 Patent, Carbyne has suffered damages in an amount not yet determined for which Carbyne is entitled to relief.

COUNT III: PATENT INFRINGEMENT OF THE ’138 PATENT

88. Carbyne incorporates by reference the preceding paragraphs as though fully set forth herein.

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

89. Apple has directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least claims 1, 3, 7-8, 10-13, 15, 19, and 22-25 of the ’138 Patent by making, testing, using, selling, and/or offering for sale its A-Series iOS devices and M-Series Macs in the United States, in violation of 35 U.S.C. § 271(a). *See* Exs. K and L.

90. Apple’s A-Series iOS devices and M-Series Macs, meet each and every element of at least claims 1, 3, 7-8, 10-13, 15, 19, and 22-25 of the ’138 Patent, either literally or equivalently.

91. Apple has had actual and/or constructive knowledge of the existence of the ’138 Patent since no later than the filing of this Original Complaint.

92. With knowledge of the ’138 Patent, at least as of the Complaint, Apple has indirectly infringed one or more claims thereof under 35 U.S.C. § 271(b) through the active inducement of direct infringement by intending to encourage, and in fact encouraging others to install software updates on the A-Series iOS devices and M-Series Macs sold and used within the United States in an infringing manner that practiced the inventions claimed by the ’138 Patent, including at least claims 1, 3, 7-8, 10-13, 15, 19, and 22-25. Apple has actively induced such direct infringement through its communications with customers, thereby providing, *inter alia*, functionality, instructions, and other assistance that have served to facilitate, promote, and cause users of Apple A-Series iOS devices and M-Series Macs, and potentially others yet unknown, to directly infringe at least claims 1, 3, 7-8, 10-13, 15, 19, and 22-25 of the ’138 Patent, as described in Exs. K and L. Upon information and belief, Apple has performed the acts that constitute inducement of infringement with the knowledge or willful blindness that the resulting acts induced thereby would constitute direct infringement by users of Apple A-Series iOS devices and M-Series Macs, and/or potentially by others as yet unknown.

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

93. As a direct and proximate consequence of Apple's infringement of the '138 Patent, Carbyne has suffered damages in an amount not yet determined for which Carbyne is entitled to relief.

COUNT IV: PATENT INFRINGEMENT OF THE '010 PATENT

94. Carbyne incorporates by reference the preceding paragraphs as though fully set forth herein.

95. Apple has directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least claims 1, 5, 6, 9, 13, 14, 17 and 21-22 of the '010 Patent by making, testing, using, selling, and/or offering for sale its A-Series iOS devices in the United States, in violation of 35 U.S.C. § 271(a). *See* Ex. M.

96. Apple's A-Series iOS devices meet each and every element of at least claims 1, 5, 6, 9, 13, 14, and 17 of the '010 Patent, either literally or equivalently.

97. Apple has had actual and/or constructive knowledge of the existence of the '010 Patent since no later than the filing of this Original Complaint.

98. With knowledge of the '010 Patent, at least as of the Complaint, Apple has indirectly infringed one or more claims thereof under 35 U.S.C. § 271(b) through the active inducement of direct infringement by intending to encourage, and in fact encouraging others to install software updates on the A-Series iOS devices sold and used within the United States in an infringing manner that practiced the inventions claimed by the '010 Patent, including at least claims 1, 5, 6, 9, 13, 14, 17 and 21-22. Apple has actively induced such direct infringement through its communications with customers, thereby providing, *inter alia*, functionality, instructions, and other assistance that have served to facilitate, promote, and cause users of Apple A-Series iOS devices, and potentially others yet unknown, to directly infringe at least

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

claims 1, 5, 6, 9, 13, 14, 17 and 21-22 of the ’010 Patent, as described in Ex. M. Upon information and belief, Apple has performed the acts that constitute inducement of infringement with the knowledge or willful blindness that the resulting acts induced thereby would constitute direct infringement by users of Apple A-Series iOS devices, and/or potentially by others as yet unknown.

99. As a direct and proximate consequence of Apple’s infringement of the ’010 Patent, Carbyne has suffered damages in an amount not yet determined for which Carbyne is entitled to relief.

COUNT V: PATENT INFRINGEMENT OF THE ’656 PATENT

100. Carbyne incorporates by reference the preceding paragraphs as though fully set forth herein.

101. Apple has directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least claims 1, 4, 7-10, 13, 16-19 of the ’656 Patent by making, testing, using, selling, and/or offering for sale its A-Series iOS devices in the United States, in violation of 35 U.S.C. § 271(a). See Ex. N.

102. Apple’s A-Series iOS devices, meet each and every element of at least claims 1, 4, 7-10, 13, 16-19 of the ’656 Patent, either literally or equivalently.

103. Apple has had actual and/or constructive knowledge of the existence of the ’656 Patent since no later than the filing of this Original Complaint.

104. With knowledge of the ’656 Patent, at least as of the Complaint, Apple has indirectly infringed one or more claims thereof under 35 U.S.C. § 271(b) through the active inducement of direct infringement by intending to encourage, and in fact encouraging others to install software updates on the A-Series iOS devices sold and used within the United States in an

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

infringing manner that practiced the inventions claimed by the ’656 Patent, including at least claims 1, 4, 7-10, 13, 16-19. Apple has actively induced such direct infringement through its communications with customers, thereby providing, inter alia, functionality, instructions, and other assistance that have served to facilitate, promote, and cause users of Apple A-Series iOS devices, and potentially others yet unknown, to directly infringe at least claims 1, 4, 7-10, 13, 16-19 of the ’656 Patent, as described in Ex. N. Upon information and belief, Apple has performed the acts that constitute inducement of infringement with the knowledge or willful blindness that the resulting acts induced thereby would constitute direct infringement by users of Apple A-Series iOS devices, and/or potentially by others as yet unknown.

105. As a direct and proximate consequence of Apple’s infringement of the ’656 Patent, Carbyne has suffered damages in an amount not yet determined for which Carbyne is entitled to relief.

COUNT VI: PATENT INFRINGEMENT OF THE ’886 PATENT

106. Carbyne incorporates by reference the preceding paragraphs as though fully set forth herein.

107. Apple has directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least claims 1-2, 4-7, 9-11, 12, 14, 18, and 20 of the ’886 Patent by making, testing, using, selling, and/or offering for sale its A-Series iOS devices in the United States, in violation of 35 U.S.C. § 271(a). See Ex. O.

108. Apple’s A-Series iOS devices, meet each and every element of at least claim 1 of the ’886 Patent, either literally or equivalently.

109. Apple has had actual and/or constructive knowledge of the existence of the ’886 Patent since no later than the filing of this Original Complaint.

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

110. With knowledge of the ’886 Patent, at least as of the Complaint, Apple has indirectly infringed one or more claims thereof under 35 U.S.C. § 271(b) through the active inducement of direct infringement by intending to encourage, and in fact encouraging others to install software updates on the A-Series iOS devices sold and used within the United States in an infringing manner that practiced the inventions claimed by the ’886 Patent, including at least claims 1-2, 4-7, 9-11, 12, 14, 18, and 20. Apple has actively induced such direct infringement through its communications with customers, thereby providing, inter alia, functionality, instructions, and other assistance that have served to facilitate, promote, and cause users of Apple A-Series iOS devices, and potentially others yet unknown, to directly infringe at least claims 1-2, 4-7, 9-11, 12, 14, 18, and 20 of the ’886 Patent, as described in Ex. O. Upon information and belief, Apple has performed the acts that constitute inducement of infringement with the knowledge or willful blindness that the resulting acts induced thereby would constitute direct infringement by users of Apple A-Series iOS devices, and/or potentially by others as yet unknown.

111. As a direct and proximate consequence of Apple’s infringement of the ’886 Patent, Carbyne has suffered damages in an amount not yet determined for which Carbyne is entitled to relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for the following relief:

112. Entry of judgment declaring that Apple has directly infringed, and/or induced others to infringe with regard to one or more claims of each of the Asserted Patents.

113. An order awarding damages sufficient to compensate Carbyne for Apple’s infringement of the Asserted Patents, but in no event less than a reasonable royalty, including

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

supplemental damages post-verdict, together with pre-judgment and post-judgment interest and costs;

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

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

116. An accounting for acts of infringement;

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

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

DEMAND FOR JURY TRIAL

Carbyne demands a trial by jury of any and all issues triable of right before a jury, except for future patent infringement, which is an issue in equity to be determined by the Court.

APPLE EXHIBIT 1056
APPLE v. PROXENSE
IPR2024-00783

Dated: March 24, 2023.

MCKOOL SMITH, P.C.

/s/ *Joshua W. Budwin*

Joshua W. Budwin
Lead Attorney
Texas State Bar No. 24050347
jbudwin@mckoolsmith.com
George T. Fishback, Jr.
Texas State Bar No. 24120823
gfishback@McKoolSmith.com
Caroline Burks
Texas State Bar No. 24126000
cburks@McKoolSmith.com
MCKOOL SMITH, P.C.
303 Colorado Street Suite 2100
Austin, TX 78701
Telephone: (512) 692-8700
Telecopier: (512) 692-8744

Richard A. Kamprath
Texas State Bar No. 24078767
rkamprath@McKoolSmith.com
Bradley Jarrett
Texas State Bar No. 24128518
bjarrett@mckoolsmith.com
MCKOOL SMITH, P.C.
300 Crescent Court, Suite 1500
Dallas, TX 75201
Telephone: (214) 978-4210

ATTORNEYS FOR PLAINTIFF CARBYNE BIOMETRICS, LLC