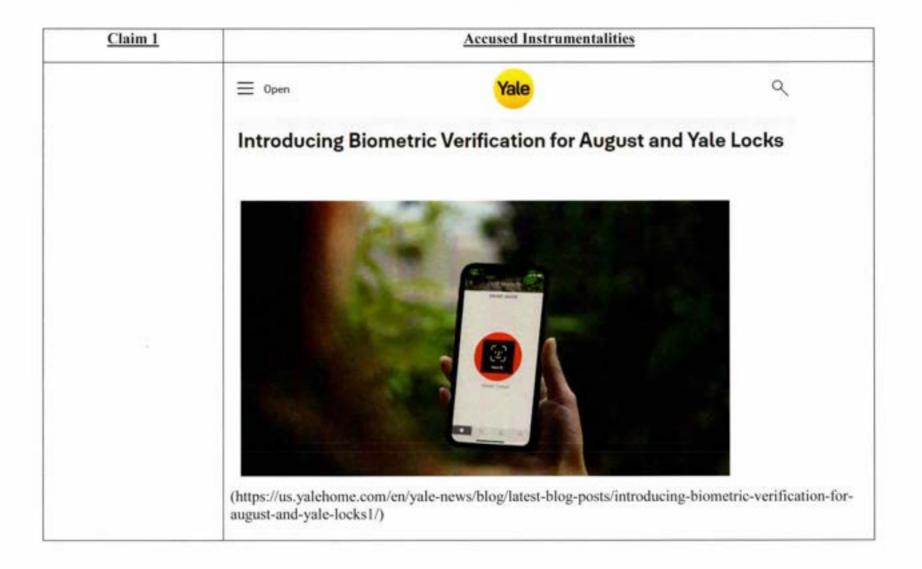
#### Claim Chart for U.S. Patent No. 9,665,705 ("the '705 Patent")

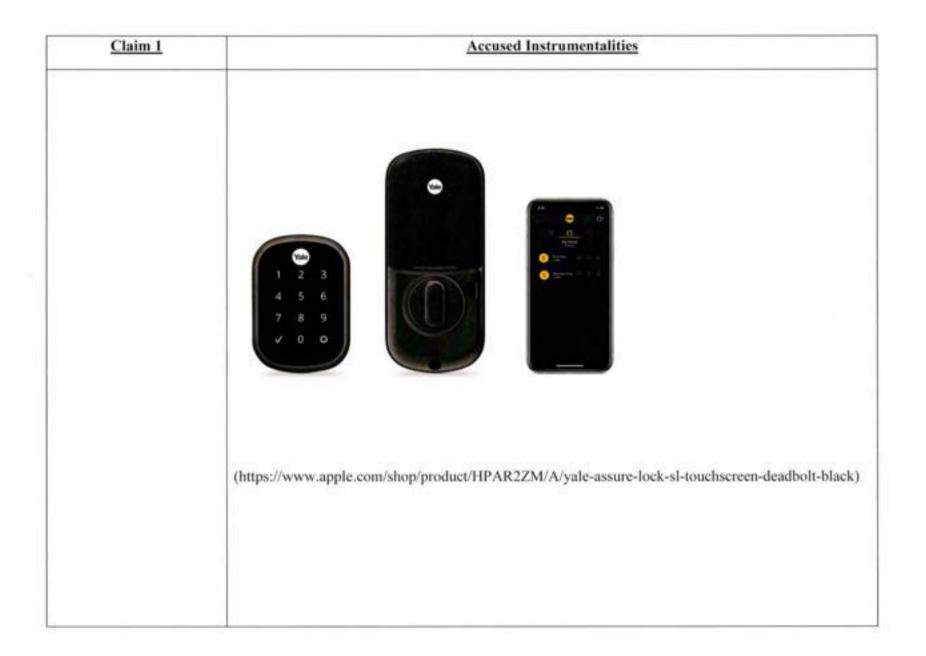
The Accused Instrumentalities include, but are not necessarily limited to, Apple iPhone and Apple iPad compatible with Yale Smart Locks, and any Apple product or device that is substantially or reasonably similar to the functionality set forth below. The Accused Instrumentalities infringe the claims of the '705 Patent, as described below, either directly under 35 U.S.C. § 271(a), or indirectly under 35 U.S.C. §§ 271(b)–(c). The Accused Instrumentalities infringe the claims of the '705 Patent literally and, to the extent not literally, under the doctrine of equivalents.

Claim 1	Accused Instrumentalities
<ol> <li>A system for providing secure access to a controlled item, the</li> </ol>	To the extent that the preamble is deemed to be a limitation, the Accused Instrumentalities are configured to use a system in accordance with this claim.
controlled item, the system comprising:	More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.
	"When the "Secure Remote Access" feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it." (https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/)

### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 3 of 232



Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 4 of 232



ASSA ABLOY Ex. 1021 - Page 3 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 5 of 232

<u>Claim 1</u>	Accused Instrumentalities	
	The Accused Instrumentalities compatible with Yale Smart Locks are shown below: Compatibility	
	iPhone Models     iPad Models       iPhone 12 Pro     (Pad Por 12.9-inch       iPhone 12 Pro     (Pad Por 12.9-inch       iPhone 12 mini     iPad Por 12.9-inch       iPhone 12     iPad Por 12.9-inch       iPhone 12     iPad Por 12.9-inch       iPhone 11     iPad Por 12.9-inch       iPhone 11 Pro     iPad Por 12.9-inch       iPhone 11 Pro     iPad Por 12.9-inch       iPhone 11     iPad generation       iPhone SE (2nd generation)     iPad Por 12.9-inch       iPhone XS     (Pad Pro 11.5-inch       iPhone X     iPad Pro 11.5-inch       iPhone 8     (Pad Pro 15.5-inch       iPhone 7     iPad Pro 10.5-inch       iPhone 6s     iPad Ari (3td generation)       iPhone 6s     iPad Ari (3td generation)       iPhone 6s     iPad Ari (3td generation)       iPad Ari (3td generation)       iPad (Ari generation)	
1a. a memory comprising a database of biometric signatures;	The Accused Instrumentalities include a memory comprising a database of biometric signatures.	

ASSA ABLOY Ex. 1021 - Page 4 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 6 of 232

<u>Claim 1</u>	Accused Instrumentalities	
	More specifically, the iPhone allows multiple biometric signatures to be entered into a database on the iPhone: Touch ID The iPhone allows the registration of multiple fingerprints:	
	Image: Source of the second of th	
	Fig. from https://support.apple.com/en-us/HT201371 under Manage Touch ID Settings. In the second bullet, it literally says:	
	"Register up to five fingerprints."	
	"Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device."	

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 7 of 232

Claim 1	Accused Instrumentalities	
	(https://support.apple.com/en-us/HT204587)	
	"Touch ID can read multiple fingerprints and recognize fingerprints at any orientation of the finger. The system then creates a mathematical representation of your fingerprint and compares it to the registered fingerprint data to determine a match and unlock your device." (https://support.apple.com/en-us/HT204587)	
	Face ID	
	The iPhone allows the registration of multiple faces:	
	Image: Section of the section of th	
	To register a face, the iPhone takes a series of pictures of the user in different poses while circling hi head. This is revealed in detail in https://support.apple.com/en-us/HT208109 in the second section "Configure Face ID", there also the figure shown above.	

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 8 of 232

<u>Claim 1</u>	Accused Instrumentalities
	To register a second face, the iPhone offers a corresponding option in its settings. If the user selects the option "Set up an alternative appearance" as shown in the figure below (from How To Add A Second Face To Face ID - Macworld UK; https://www.macworld.co.uk/how-to/second-face-id-3803421/), a second face is registered by the iPhone in the same way as the first face. "Set up Face ID or add another face. • Select "Settings" > "Face ID & Code" > "Configure alternate appearance" if you want to configure another face to be recognized by Face ID." (https://support.apple.com/de-de/guide/iphone/iph6d162927a/ios)

### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 9 of 232

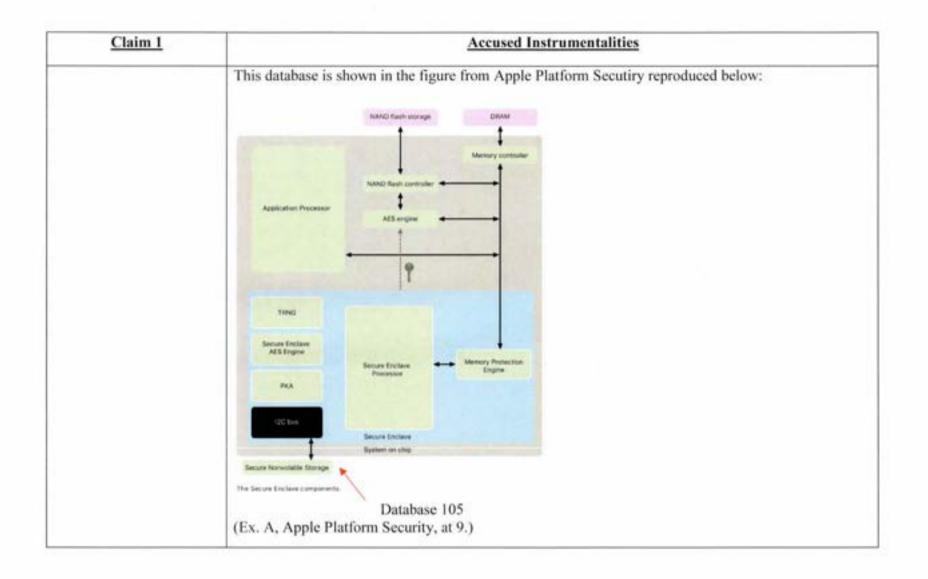
Claim 1	Accused Instrumentalities		
	Simma Face ID & Passcode		
	Phone Unlock		
	(Tures App Store		
	Acol		
	Passwort LutoFill		
	Other Act # Apps 1		
	Affairer can a construction, development of memory and a second s		
	Final ET & Private L		
	Set Up an Alternative Approximitie		
	N addition is contributed by thermal has point bank. Face the law resultance an adversaries appendices		
	Reset Face 10		
	6/7339-73249-		
	Require Attention for Face ID		
	The page How To Add A Second Face To Face ID - Macworld UK		
	(https://www.macworld.co.uk/how-to/second-face-id-3803421/) literally states:		
	"Face ID is a fast and secure way to unlock your iPhone or iPad Pro, but you may not know that you can actually set up more than one face to use the feature.		
	This second face could belong to a loved one, enabling your partner or child to access your phone without requiring your smiling mug to unlock it. "		
	To store the biometric signatures ("template data") from the received biometric signals, the iPhone has a System on Chip (SOC) called a Secure Enclave. A Secure Enclave Processor provides the Secure Enclave with computing power:		

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 10 of 232

<u>Claim 1</u>	Accused Instrumentalities
	"The Secure Enclave is a system on chip (SoC) that is included on all recent iPhone, devices" (Ex. A, Apple Platform Security, at 7.)
	"The Secure Enclave is a dedicated secure subsystem integrated into Apple systems on chip (SoCs)." ( <i>Id.</i> , at 9.)
	The Secure Enclave Processor provides the main computing power for the Secure Enclave." ( <i>Id.</i> , at 10.)
	"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." ( <i>Id.</i> , at 19.)
	The Secure Enclave has access to a memory assigned to it and accessible only to it:
	Secure nonvolatile storage "The Secure Enclave is equipped with a dedicated secure nonvolatile storage device. The secure nonvolatile storage is connected to the Secure Enclave using a dedicated I2C bus, so that it can only be accessed by the Secure Enclave." ( <i>Id.</i> , at 15.)
	This memory serves as a database for storing the biometric signatures:
	"The secure nonvolatile storage is used for all anti-replay services in the Secure Enclave. Anti-replay services on the Secure Enclave are used for revocation of data over events that mark anti-replay boundaries including, but not limited to, the following:
	<ul> <li></li> <li>Adding or removing a Touch ID fingerprint or Face ID face".</li> </ul>
	( <i>Id.</i> , at 16.)

ASSA ABLOY Ex. 1021 - Page 9 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 11 of 232



ASSA ABLOY Ex. 1021 - Page 10 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

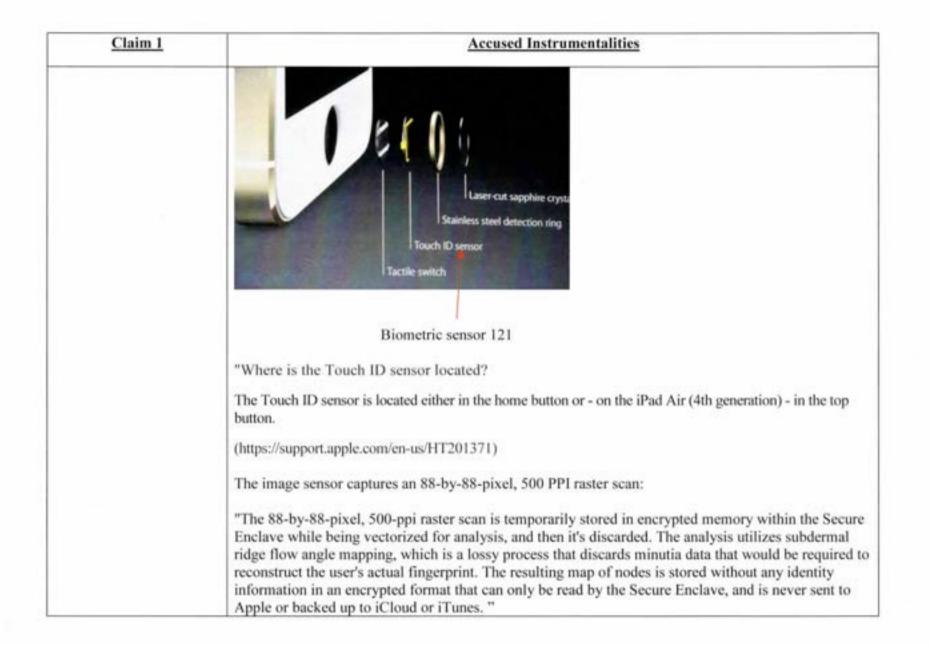
### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 12 of 232

Claim 1	Accused Instrumentalities	
<ol> <li>a transmitter sub- system comprising:</li> </ol>	As set forth in elements 1b1, 1b2, and 1b3 below, the Accused Instrumentalities include a transmitter sub-system.	
	The iPhone's Secure Enclave is a transmitter sub-system. It sends ephemerally re-encrypted file keys to the application processor with its file system driver ("Application Processor file-system driver") to read the files in the NAND Flash Storage.	
	NAND Rush storage DRAM	
	Memory contrailer	
	Adminution Processor	
	• •	
	TING	
	Secure Enclave ALS Engine Secure Enclave Memory Presention	
	Processor Processor	
	CC ture  Secure Enclave  Splatem on shea	
	Secure Nonvolatile Etorage The Secure Enclave components.	
	(Ex. A, Apple Platform Security, at 9.)	

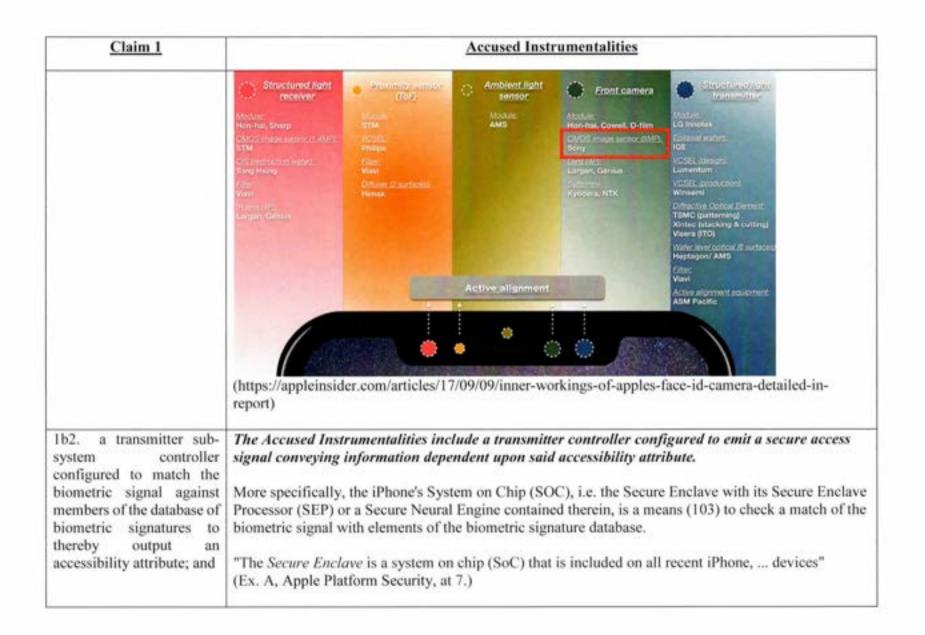
### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 13 of 232

	Accused Instrumental	ities
	When the file-system driver	e keys for use by the Application reads or writes a file, it sends the
the Application Processor. [ ]		the file key is never directly exposed to raps a file's keys, they're rewrapped wit or."
The file system driver of the a	pplication processor is an NVM	IE driver:
Filesystem Data Protection		
User	Kernel	SEP
	L Fetch wrapped	
apen("foa.txt",)	netadata	Kiny Store     Z. University for key using keybing key
apen("foa.txt",)	t le, key from HDS +	Key Store     Z. Unweap to Arry     using keybing key      AES Engine     AES Engine     S. Wrap file, key using     ephemeral key,     rebarn ephemerally     wrapped file, key     to kernel

<u>Claim 1</u>	Accused Instrumentalities
1b1. a biometric sensor configured to receive a	The Accused Instrumentalities include a biometric sensor configured to receive a biometric signal.
biometric signal;	More specifically, the iPhone has at least one biometric sensor for capturing a fingerprint or a face (Touch ID and/or Face ID), namely a Touch ID sensor and a camera system with image sensor, respectively.
	Touch ID
	"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.)
	"Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the <b>sensor</b> continuing to expand the fingerprint map as additional overlapping nodes are identified with each use." ( <i>Id.</i> )
	"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave." ( <i>Id.</i> )
	The biometric sensor for Touch ID is located below the home button:
	"The Home button is a stack of different materials, capped with a sapphire crystal lens. The surrounding stainless-steel ring works as a ground and detects the user's finger. This action activates a capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors." (https://appleinsider.com/inside/touch-id)



Claim 1	Accused Instrumentalities
	(Ex. C, iOS Security white paper, at 8.)
	Face ID
	The biometric sensor for facial biometrics is a camera system (" <b>TrueDepth</b> camera <b>system</b> ") with an image sensor.
	"With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face." (Ex. A, Apple Platform Security, at 20.)
	To receive a biometric signal, the camera system with image sensor reads over 30,000 infrared points to capture depth information along with a two-dimensional infrared image.
	"After the TrueDepth camera confirms the presence of an attentive face, it projects and <b>reads over</b> <b>30,000 infrared dots to form a depth map of the face along with a 2D infrared image</b> . This data is used to <b>create a sequence of 2D images and depth maps</b> , which are digitally signed and sent to the Secure Enclave. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." ( <i>Id.</i> )
	The camera system includes a biometric image sensor, namely a "CMOS image" sensor from Sony, to perform facial biometrics:



### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 18 of 232

Claim 1	Accused Instrumentalities
	"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device or respond that a match is valid (for Apple Pay, in-app, and other uses of Touch ID and Face ID). " ( <i>Id.</i> , at 19.)
	The biometric signal received from the biometric sensor ("incoming data from the biometric sensor") is thus checked by the Secure Enclave and its SEP with the elements of the database of biometric signatures 105, i.e. the "stored templates", for the presence of a match.
	For Touch ID, the Secure Enclave match verification is performed as follows:
	"The Secure Enclave is responsible for processing fingerprint data from the Touch ID sensor, determining if there is a match against registered fingerprints, and then enabling access or purchases on behalf of the user" (Ex. C, iOS Security white paper, at 7.)
	"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches" (Ex. A, Apple Platform Security, at 19.)
	"Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. " (https://support.apple.com/en-us/HT204587)
	"Touch ID can read multiple fingerprints and recognize fingerprints at any orientation of the finger. The system then creates a mathematical representation of your fingerprint and compares it to the registered fingerprint data to determine a match and unlock your device." (https://support.apple.com/de-de/HT204587)

### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 19 of 232

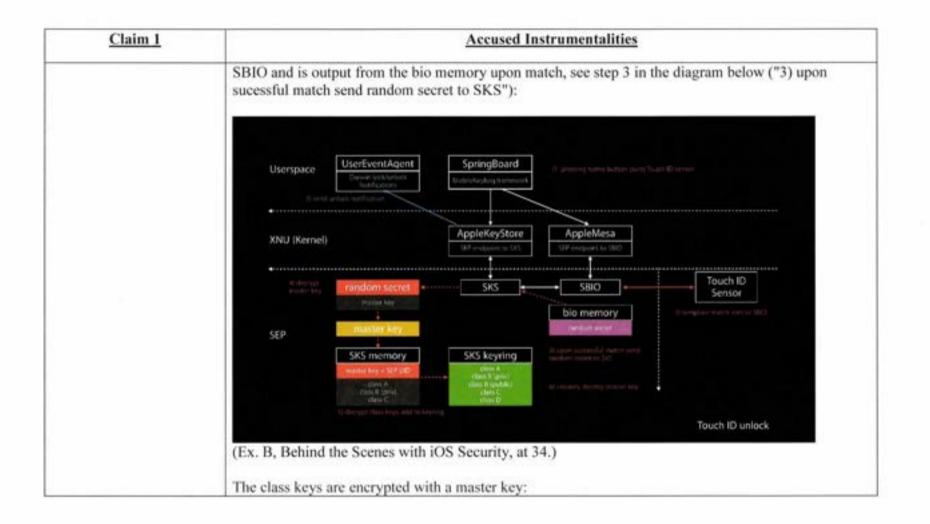
<u>Claim 1</u>	Accused Instrumentalities	
	For Face ID, the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:	
	"Face ID uses neural networks for determining attention, <b>matching</b> , and antispoofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)	
	"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." ( <i>Id.</i> ).	
	"Facial matching security	
	Facial matching is performed within the Secure Enclave using neural networks trained specifically for that purpose Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device." ( <i>Id.</i> at 23.)	
	When the Secure Enclave, or more precisely the Touch ID or Face ID subsystem within the Secure Enclave, has determined that a match exists, an accessibility attribute is issued by the corresponding Touch ID or Face ID subsystem. This Touch ID or Face ID subsystem is also referred to as the SBIO. The accessibility attribute confirms that there is a match and that the iPhone is to be unlocked (" determine whether to unlock the device").	
	This confirmation of the match is signaled by the SBIO by issuing a random secret to which only the Touch ID or Face ID subsystem within the Secure Enclave has access:	
	"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device []." ( <i>Id.</i> at 19.)	

ASSA ABLOY Ex. 1021 - Page 18 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 20 of 232

<u>Claim 1</u>	Accused Instrumentalities
	"Uses for Touch ID and Face ID
	Unlocking a device or user account
	[] keys for the highest class of Data Protection-which are held in the Secure Enclave [].
	With Touch ID or Face ID enabled, the keys aren't discarded when the device or account locks; instead, <b>they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the</b> <b>Secure Enclave</b> . When a user attempts to unlock the device or account, <b>if the device detects a</b> <b>successful match, it provides the key for unwrapping the Data Protection keys</b> , and the device or account is unlocked. This process provides additional protection by requiring cooperation between the Data Protection and Touch ID or Face ID subsystems to unlock the device."
	( <i>Id.</i> at 24.)
	"The class key is protected with the hardware UID and, for some classes, the user's passcode." ( <i>Id.</i> at 85.)
	"Complete Protection
	(NSFileProtectionComplete): The class key is protected with a key derived from the user passcode or password and the device UID. Shortly after the user locks a device (10 seconds, if the Require Password setting is Immediately), the decrypted class key is discarded, rendering all data in this class inaccessible until the user enters the passcode again or unlocks (logs in to) the device using Touch ID or Face ID."
	( <i>Id.</i> at 86.)
	The Touch ID or Face ID subsystem within the Secure Enclave is the SBIO shown below. SBIO is an application that runs within the Secure Enclave on the SEP and is responsible for checking the match of biometric features. SBIO receives the corresponding biometric data from a biometric sensor, such as the Touch ID sensor. The random secret is stored in a memory ("bio memory") associated with the

### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 21 of 232

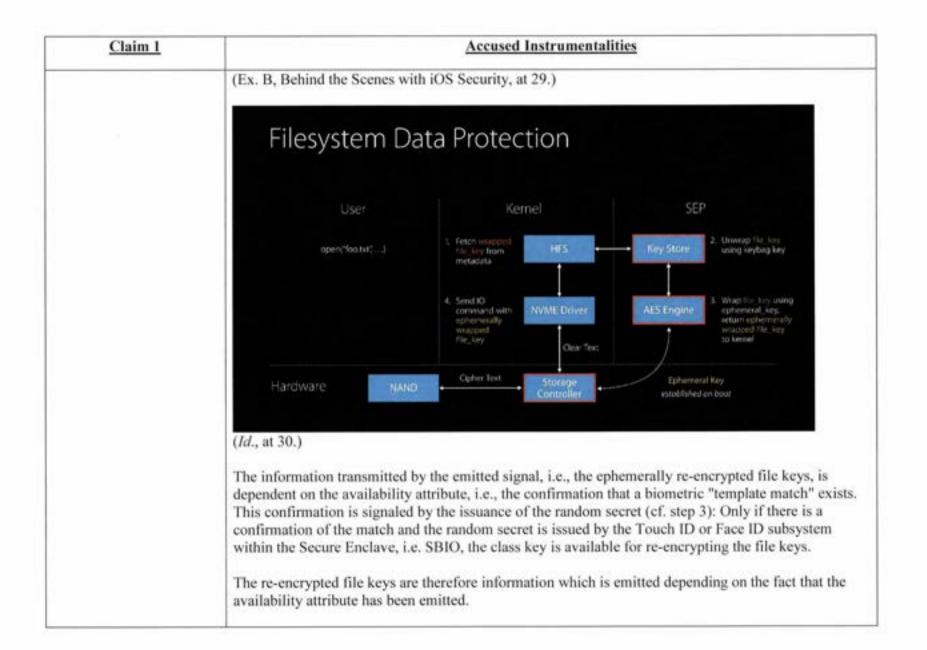


Claim 1	Accused Instrumentalities	
	User Keybags	
	Background	
	Sets of keys generated for each user to protect their data at rest	
	Keys wrapped by master key derived from user passcode and SEP UID	
	After 10 incorrect passcode entries, SEP will not process any further attempts	
	Different policy associated with each keybag key—Usage, availability	
	( <i>Id.</i> , at 25.)	
	The random secret is issued to SKS. SKS is a Secure Key Service application which is located within the Secure Enclave on the SEP and is responsible for decrypting class keys. The random secret provided by SBIO is used to decrypt a master key ("4) decrypt master key"). The master key is concatenated with the UID of the SEP and thus class keys are decrypted and added to the SKS keyring ("5) decrypt class keys, add to keyring") for further use by the Secure Enclave. The decrypted class keys include, for example, the class key of class A.	
1b3. a transmitter configured to emit a secure access signal conveying	The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.	
information dependent upon said accessibility attribute; and	For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys: "sepOS can then use the ephemeral wrapping key to wrap file keys for use by the Application Processor file-system driver. When the file-system driver reads or writes a file, it sends the wrapped key to the AES Engine."	

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 23 of 232

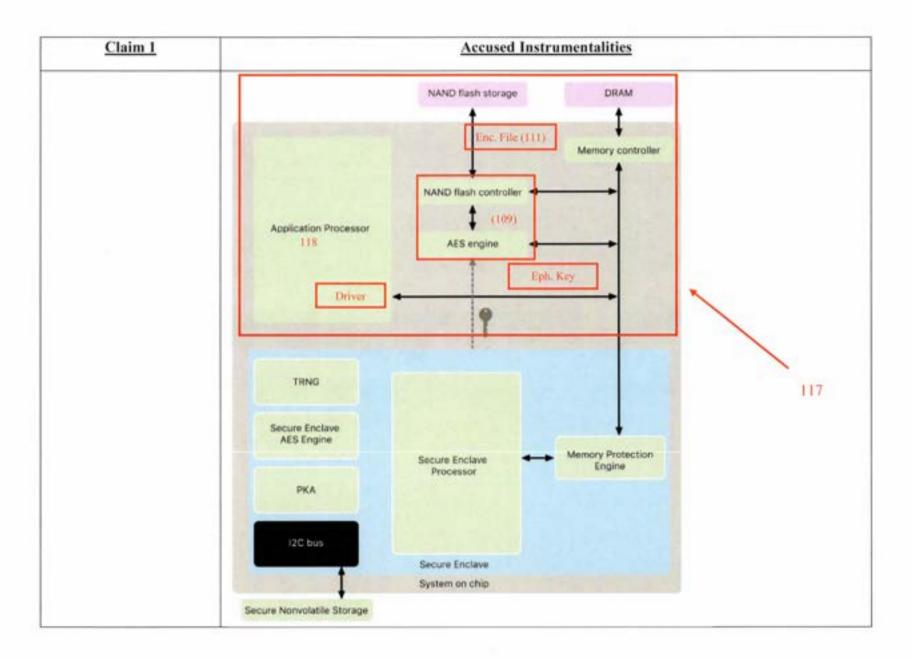
<u>Claim 1</u>	Accused Instrumentalities		
	(Ex. A, Apple Platform Security, at 14.)		
	"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. [] When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." ( <i>Id.</i> at 85.)		
	The signal with the ephemerally re-encrypted file keys is a secure signal because it comes from the Secure Enclave and thus from a secure environment. Furthermore, the signal is secure because the transmitted information is encrypted. The emitted file keys are encrypted with the ephemeral key:		
	"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. At startup, the Secure Enclave negotiates an ephemeral key with the AES Engine. When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key an sent back to the Application Processor." ( <i>Id.</i> )		
	Filesystem Data Protection		
	Overview		
	File blocks are encrypted using AES-XTS with 128-bit keys		
	Each file on the user partition is encrypted using a unique random key chosen by St		
	Raw file keys are never exposed to the AP		
	Wrapped with a key from the user keybag for long-term storage		
	<ul> <li>Wrapped with an ephemeral key while in use, bound to boot session</li> </ul>		

### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 24 of 232



<u>Claim 1</u>	Accused Instrumentalities
1c. a receiver sub-system comprising:	As set forth in elements 1c1 and 1c2 below, the Accused Instrumentalities include a receiver sub- system.
	The receiver subsystem is the part of the system outside the Secure Enclave that is responsible for reading encrypted files from the NAND Flash Storage and receives ephemerally re-encrypted file keys from the Secure Enclave for this purpose:

### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 26 of 232



ASSA ABLOY Ex. 1021 - Page 25 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

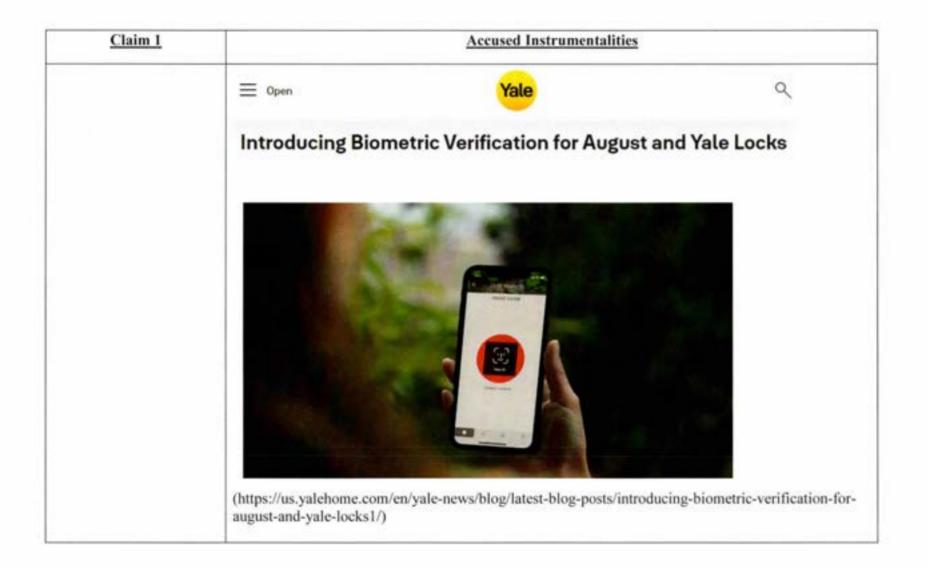
# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 27 of 232

Claim 1	Accused Instrumentalities		
	(Ex. A, Apple Platform Secur	rity, at 9.)	
1c1. a receiver sub-system controller configured to: receive the transmitted secure access signal; and	The Accused Instrumentalities include a receiver sub-system controller configured to: receive the transmitted secure access signal. An application processor (118) with file system driver, which receives the ephemerally re-encrypted file key. To read files from the NAND Flash storage, the application processor processes the received signal by creating a read command with the ephemerally wrapped file key ("IO command with ephemerally wrapped file key") and sends it to the storage controller (109) (NAND Flash controller with AES engine). This read command provides the storage controller with all the information required to read and decrypt the encrypted file from the NAND flash storage: Filesystem Data Protection		
	User	Kernel	SEP
	User opentfloatut73	Kernel	SEP 2. University file, here using keybog key
		L. Fetch wapped the key from HES	2 House the law

ASSA ABLOY Ex. 1021 - Page 26 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 28 of 232

Claim 1	Accused Instrumentalities
	"sepOS can then use the ephemeral wrapping key to wrap file keys for use by the Application Processor file-system driver. When the file-system driver reads or writes a file, it sends the wrapped key to the AES Engine." (Ex. A, Apple Platform Security, at 14.) "All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. [] When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." ( <i>Id.</i> , at 85.)
1c2. provide conditional access to the controlled item dependent upon said information;	The Accused Instrumentalities include a receiver sub-system configured to provide conditional access to the controlled item dependent upon said information. More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.
	"When the "Secure Remote Access" feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it." (https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for- august-and-yale-locks1/)



### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 30 of 232



<u>Claim 1</u>	Accused Instrumentalities
1d. wherein the transmitter sub-system controller is further configured to:	The Accused Instrumentalities include a transmitter sub-system controller that is configured to be used as set forth in elements 1d1, 1d2, and 1d3 below.
1d1. receive a series of entries of the biometric signal, said series being characterized according to	The Accused Instrumentalities include a transmitter sub-system controller configured to receive a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry.
at least one of the number of said entries and a duration of each said entry;	More specifically, the Secure Enclave of the iPhone with the Secure Enclave Processor forms the means for receiving a series of entries of the biometric signal.
duration of each said entry,	"Apple's biometric security architecture relies on a strict separation of responsibilities between the biometric sensor and the Secure Enclave, and a secure connection between the two. The sensor captures the biometric image and securely transmits it to the Secure Enclave." (Ex. A, Apple Platform Security, at 19.)
	Touch ID
	When a finger is placed on the biometric sensor, the finger is scanned and the corresponding biometric signal entry is received by the Secure Enclave.
	"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave." ( <i>Id.</i> )
	To enroll a fingerprint in the database, the iPhone's fingerprint sensor records an entry of a biometric signal when the user places his finger on the sensor. This is done multiple times, resulting in a series of entries of such biometric signals.
	Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone.

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 32 of 232

Claim 1	Accused Instrumentalities
	Set up Touch ID
	Before you can set up Touch ID, you must first create a <u>code</u> for your device,* then follow these steps: 1. Make sure the Touch ID sensor and your finger are clean and dry.
	2. Tap Settings > Touch ID & Code, and then enter your code.
	<ol><li>Tap "Add fingerprint" and hold the device as you normally would when touching the Touch ID sensor.</li></ol>
	4. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.           Image: Place Your Finger           Image: Place Your Finger
	<ol><li>Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.</li></ol>

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 33 of 232

<u>Claim 1</u>	Accused Instrumentalities
	6. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you would during the first scan."
	(https://support.apple.com/en-us/HT201371)
	Accordingly, the user is prompted to place his finger on the sensor several times, in particular in accordance with step 5. Each time the finger is placed on the sensor, a corresponding biometric entry is generated, i.e. a series of such entries. All these entries, which result from placing the same finger on the sensor, form a series.
	Face ID
	The means for receiving a series of entries of the biometric signal includes a Secure Neural Engine, which is protected by the Secure Enclave. The Secure Neural Engine transforms the series of entries of the biometric signal received by the Secure Enclave into a biometric signature ("mathematical representation").
	"After the TrueDepth camera confirms the presence of an attentive face, it projects and reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image. This data is used to create <b>a sequence of 2D images and depth maps</b> , which are digitally signed and <b>sent to the Secure Enclave</b> . To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the <b>Secure Neural Engine-protected</b> within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)
	Each entry of the biometric signal thus contains a two-dimensional infrared image with 30,000 infrared points for capturing depth information. By continuously capturing such infrared images into a Face ID scan while the user moves his head into different poses, a series of entries of the biometric signal

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 34 of 232

<u>Claim 1</u>	Accused Instrumentalities
	results. Two such Face ID scans are required to generate a biometric signature of a single face, so that two series of entries of the biometric signal are received accordingly.
	Using Face ID on iPhone
	1. Tap Settings > Face ID & Code. Enter your code when prompted.
	2. Tap on "Configure Face ID".
	3. Hold the device in portrait mode in front of your face and tap "Let's go".
	4. Make sure your face is inside the frame and slowly move your head until the circle shown is completed. If you can't move your head, tap on "Options for operating aids".
	5. After performing the first Face ID scan, tap "Next".
	6. Again, slowly describe a circle with your head until it is completed.
	7. Tap "Done."
	(https://support.apple.com/en-us/HT208109)
	The biometric signature of a single face is thus determined by two successive Face ID scans, each of which receives a series of entries of the biometric signal (compare steps 4. and 6. above).
	To register a second face, the iPhone offers a corresponding option in its settings. If the user selects the option "Set up an alternative appearance" as shown in the figure below on https://www.macworld.co.uk/how-to/second-face-id-3803421/, a second face is registered by the iPhone in the same way as the first face.

### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 35 of 232

Claim 1	Accused Instrumentalities	
	C Setteme Fece ID & Passcode	
	unter medit di hotee	
	Phone Unlock	
	iTuures App Store	
	Apple	
	Passwo utoFill	
	Other Act 4 Augus	
	Affinite static and the second s	
	Bet Up an Alternative Appearance	
	In addition to contravously intervent from you look. Farm It is not comprised on alternative approximation.	
	Heset Face (D	
	ATTENDO	
	Require Attention for Face ID	
	The second second second is identified on the Discussion has been and	
	The series of entries of the biometric signal is identified on the iPhone by both the number and	
	duration of each such entry.	
	Touch ID	
	According to step 5 of the instructions https://support.apple.com/en-us/HT201371, for the enrollment	
	of a single finger, the user has to repeatedly place the respective finger on the sensor and thus a number	
	of entries in a row predetermined via the user guidance are captured by the iPhone. Each one of the	
	entries must also be of a predetermined duration given to the user via the iPhone display, i.e. the user's	
	finger must remain on the sensor for a predetermined duration for each entry of the biometric signal in	
	order to capture the biometric signal during this time.	

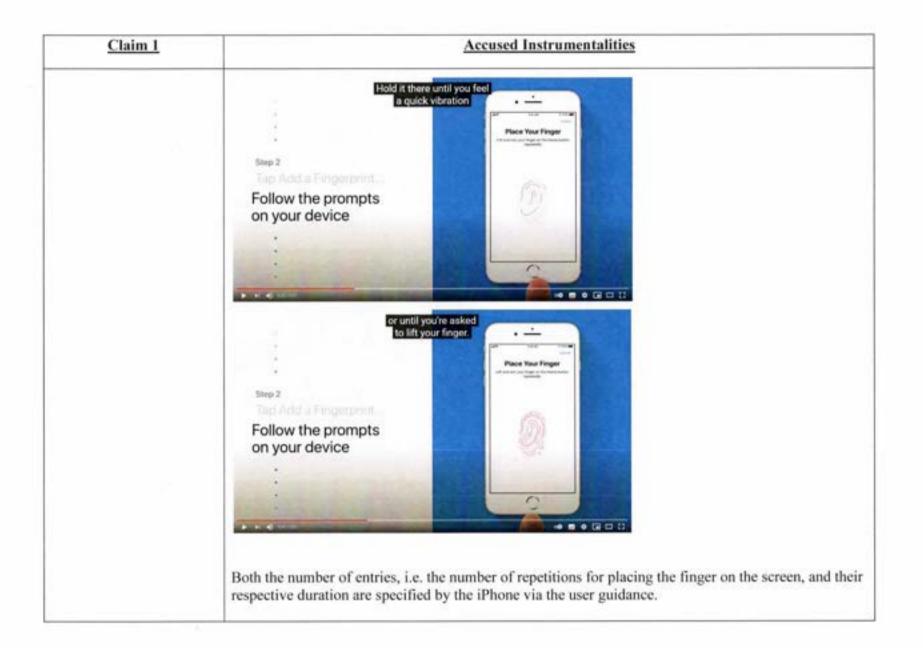
# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 36 of 232

<u>Claim 1</u>	Accused Instrumentalities
	Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone and iPad.
	Set up Touch ID
	<ul> <li>4. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</li> </ul>
	uni V Buttadu Nork men Currue
	Place Your Finger Lift and rest your froger on the Home button repeatedly.
	5. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.
	6. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you did during the first scan.
	(https://support.apple.com/en-us/HT201371)

### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 37 of 232

<u>Claim 1</u>	Accused Instrumentalities
	After placing a finger on the home button, a fingerprint appears on the display with red progress bars spreading along some of the papillary bars until the capture of the biometric entry in question is complete:
	Cance
	When the required duration is reached, the iPhone vibrates after an entry of the biometric signal is received or it issues a prompt to the user to lift the finger. The user then lifts the finger in question and replaces the same finger so that the iPhone receives a series of biometric signal entries of sufficient duration for that finger. The process is repeated for the same finger for as long as required according to the iPhone's user guidance.
	This is shown in the Apple You Tube video (32) How to set up Touch ID on your iPhone or iPad - Apple Support - YouTube (https://www.youtube.com/watch?v=xTZ2LALWZlg):

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 38 of 232



ASSA ABLOY Ex. 1021 - Page 37 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 39 of 232

Claim 1	Accused Instrumentalities
	Face ID The user moves his face in front of the camera to strike different poses, and the camera system with image sensor continuously captures a large number of biometric entries, i.e. here the 2D images with depth information, in a row.
	"This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)
	The sufficient duration of an entry for a pose, i.e. an angular position of the head specified via the user interface of the iPhone, is indicated to the user by the transformation of a gray line into a green line:
	Move your head slowly to complete the circle.
	(Individual images taken from: https://support.apple.com/en-us/HT208109)

ASSA ABLOY Ex. 1021 - Page 38 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

<u>Claim 1</u>	Accused Instrumentalities
1d2. map said series into an instruction; and	The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.
	More specifically, the Secure Enclave of the iPhone contains means to assign the received row to an instruction: The Secure Enclave, after receiving the full set of entries of the biometric signal, assigns this set to an instruction for processing, encrypting and storing the biometric signature ("Touch ID and Face ID template data").
	"The sensor captures the biometric image and securely transmits it to the Secure Enclave. During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Ex. A, Apple Platform Security, at 19.)
	To carry out this instruction, the Secure Enclave has its own processor: "The Secure Enclave Processor provides the main computing power for the Secure Enclave." ( <i>Id.</i> , at 10.)
	Touch ID
	The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.
	"The analysis uses subdermal ridge flow angle mapping, a lossy process that discards "finger minutiae data" that would be required to reconstruct the user's actual fingerprint. During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches, but without any identity information." ( <i>Id.</i> , at 19.)
	Face ID

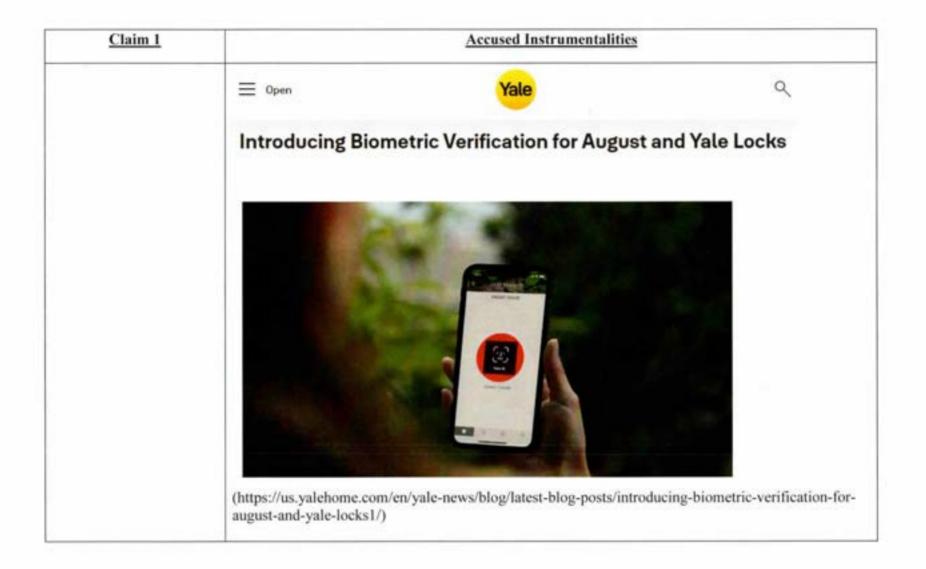
## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 41 of 232

<u>Claim 1</u>	Accused Instrumentalities
	The instruction involves the transformation of the set of entries of the biometric signal captured via the Face ID scans into a mathematical representation, i.e. the biometric signature of the face in question by the Secure Neural Engine of the Secure Enclave, as well as its encryption and storage.
	"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses. " ( <i>Id.</i> , at 20.)
	"Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device. It's not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:
	The mathematical representations of a user's face calculated during enrollment    "     ( <i>Id.</i> , at 23.)

Cla	<u>im 1</u>		Accused Instrumentalities
1d3. populat according	e the da to	tabase the	The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.
instruction,			More specifically, the Secure Enclave stores the biometric signature, i.e. the encrypted mathematical representation of the fingerprint or face, in the database 105, i.e. the "secure nonvolatile storage":
			"The secure nonvolatile storage is used for all anti-replay services in the Secure Enclave. Anti-replay services on the Secure Enclave are used for revocation of data over events that mark anti-replay boundaries including, but not limited to, the following:
			•
			<ul> <li>Adding or removing a Touch ID fingerprint or Face ID face".</li> <li>(Ex. A, Apple Platform Security, at 16.)</li> </ul>
			"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." ( <i>Id.</i> , at 19.)
			Touch ID
			"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches" ( <i>Id.</i> )
			Face ID
			The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:
			• The mathematical representations of a user's face calculated during enrollment". ( <i>Id.</i> , at 23.)

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 43 of 232

Accused Instrumentalities
The Accused Instrumentalities are configured to provide access to the controlled item, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.
More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.
"When the "Secure Remote Access" feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it." (https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-
august-and-yale-locks1/)



### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 45 of 232

<u>Claim 1</u>	Accused Instrumentalities
	(https://www.apple.com/shop/product/HPAR2ZM/A/yale-assure-lock-sl-touchscreen-deadbolt-bla

Claim 2	Accused Instrumentalities
2. The system according to claim 1, wherein the transmitter sub-system	Upon information and belief, the Accused Instrumentalities include the transmitter sub-system controller that is configured to be used as set forth in elements 2a, 2b, and 2c below.

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 46 of 232

<u>Claim 2</u>	Accused Instrumentalities
controller is further configured to:	
2a. provide a signal for directing input of the series of entries of the biometric	Upon information and belief, the Accused Instrumentalities are configure to provide a signal for directing input of the series of entries of the biometric signal.
signal;	More specifically, the Accused Instrumentalities provide instructions for the user to input a series of fingerprint or face images via Touch ID and Face ID.
	Touch ID: Register a fingerprint for Apple Touch ID by the user tapping a finger several times on the home button to record the fingerprint data.
	(https://video.search.yahoo.com/yhs/search?fr=yhs-pty-pty_ converter&hsimp=yhs- pty_converter&hspart=pty&p=registering+fingerprint+apple+touch+id+on+screen+instructions#id =1&vid=156de65ae06ca453643009fc0ea9cf79&action=click.)
	Touch ID: The user's finger must remain on the home button long enough for the data to be recorded. "Touch the Touch ID sensor with your finger, but don't press it. Hold it there until you feel a quick vibration, or until you're asked to lift your finger." "Continue to lift and rest your finger slowly, making small adjustments to the position of your finger each time." (https://support.apple.com/en-au/HT201371)
	Touch ID: "you shouldn't tap too quickly or move your finger around" (https://support.apple.com/en-us/HT207537)
	Face ID: Setting up Face ID requires two scans of the user's face. Each scan asks users to move their head slowly in a circle to register different angles of the user's face. (https://www.imore.com/how-set-face-id-iphone)

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 47 of 232



Claim 2	Accused Instrumentalities
	Image: state
2b. incorporate into the secure access signal an identification field identifying the biometric signal if the signal matches a member of the database; and	<ul> <li>(https://support.apple.com/en-us/HT208109)</li> <li>Upon information and belief, the Accused Instrumentalities are configure to incorporate into the secure access signal an identification field identifying the biometric signal if the signal matches a member of the database.</li> <li>More specifically, upon information and belief, the Accused Instrumentalities are configured to provide secure access signal when the fingerprint or face image received via Touch ID and Face ID matches the fingerprint and face data stored in the Secure Nonvolatile Storage.</li> <li>"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device or respond that a match is valid (for Apple Pay, in-app, and other uses of Touch ID and Face ID). The architecture supports devices that include both the sensor and Secure Enclave (such as iPhone, iPad, and many Mac systems), as well as the ability to physically separate the sensor into a peripheral that is then securely paired to the Secure Enclave in a Mac with Apple silicon."</li> <li>(https://support.apple.com/ko-kr/guide/security/sec067eb0c9e/1/web/1)</li> </ul>

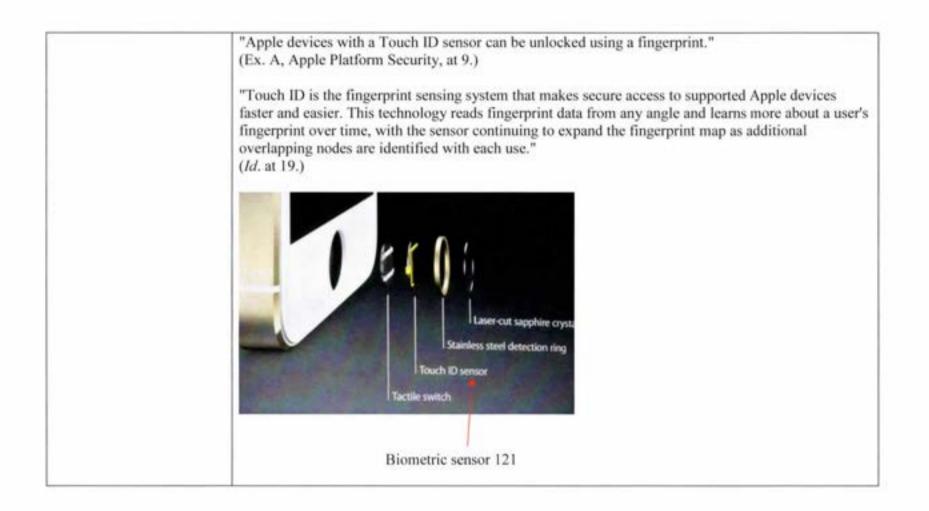
# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 49 of 232

Claim 2	Accused Instrumentalities
	With Touch ID and Face ID, the keys for the highest class of Data Protection are held in the Secure Enclave,"[w]hen a user attempts to unlock the device or account, if the device detects a successful match, it provides the key for unwrapping the Data Protection keys, and the device or account is unlocked." (Ex. A, Apple Platform Security, at 24.)
2c. construct an audit trail of biometric signals provided to the biometric sensor in order to access the controlled item.	Upon information and belief, the Accused Instrumentalities are configure to construct an audit trail of biometric signals provided to the biometric sensor in order to access the controlled item. More specifically, upon information and belief, the Accused Instrumentalities are configured to construct an audit trail of the enrolled fingerprint and face data to continually improve matching accuracy.
	"Touch ID will incrementally update the mathematical representation of enrolled fingerprints over time to improve matching accuracy." (https://support.apple.com/en-us/HT204587)
	"Face ID data - including mathematical representations of your face - is encrypted and protected by the Secure Enclave. This data will be refined and updated as you use Face ID to improve your experience, including when you successfully authenticate. Face ID will also update this data when it detects a close match but a passcode is subsequently entered to unlock the device." (https://support.apple.com/en-us/HT208108)
	In an alternative read, upon information and belief, every time a user uses Touch ID or Face ID to access an iPhone, the iPhone keeps a record of fingerprint and face unlocking, or some kind record for subsequent auditing.

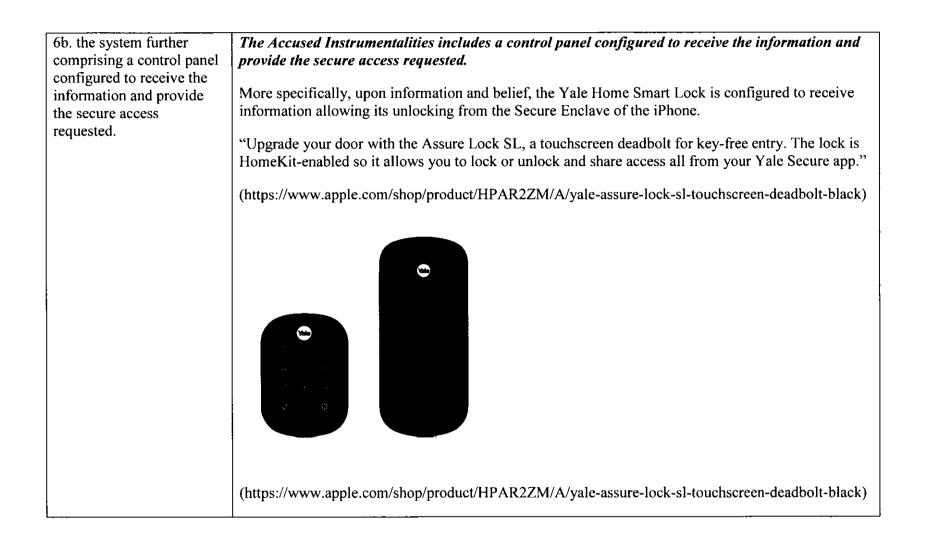
Claim 4	Accused Instrumentalities
4. The system according to claim 1, wherein the biometric sensor is responsive to one of voice, retinal pattern, iris pattern, face pattern, and palm configuration, and/or the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system.	The Accused Instrumentalities includes a biometric sensor that is responsive to one of voice, retinal pattern, fris pattern, face pattern, and palm configuration, and/or the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system. More specifically, the Accused Instrumentalities include a CMOS image sensor in the front camera of the iPhones that is responsive to face pattern of the user. Upon information and belief, the Secure Nonvolatile Storage is a memory including a database of the face data.  Face ID The biometric sensor for facial biometrics is a camera system ("TrueDepth camera system") with an image sensor.  With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face." (Ex. A, Apple Platform Security, at 20.)  (might be added in the face attern of the transmitter of the transmitter set of the secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face." (Ex. A, Apple Platform Security, at 20.)  (might be added in the secure set of the secure

Claim 6	Accused Instrumentalities
6. The system as claimed in claim 1, wherein the biometric sensor is further configured to authenticate the identity of a user;	The Accused Instrumentalities includes a biometric sensor that is further configured to authenticate the identity of a user.         More specifically, the iPhones uses Face ID and Touch ID to authenticate the user's identity.         Face ID         The biometric sensor for facial biometrics is a camera system ("TrueDepth camera system") with an image sensor.         "With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face. "         (Ex. A, Apple Platform Security, at 20.)
	Image: second

### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 52 of 232



6a. wherein the transmitter is further configured to transmit information capable of granting access to the controlled item using a secure wireless signal dependent upon a request from the user and the authentication of the user identity; and	The Accused Instrumentalities includes a transmitter configured to transmit information capable of granting access to the controlled item using a secure wireless signal dependent upon a request from the user and the authentication of the user identity.
	Upon information and belief, the Secure Enclave of the iPhone is configured to grant access to the controlled item (e.g., a locking mechanism of the door lock) via Wi-Fi, mobile data or Bluetooth dependent upon the user's request to unlock and the user's authentication via Touch ID or Face ID.
	"When the 'Secure Remote Access' feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it." "The feature applies to operations done via Wi-Fi, mobile data or Bluetooth. You'll be able to opt in to this security feature, and it will not be enacted when checking your lock status in order to preserve a seamless app experience."
	(https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for- august-and-yale-locks1/)



Claim 9	Accused Instrumentalities
9. The system according to claim 1, wherein: the transmitter sub-system and the receiver sub-system are collocated in the electronic computing device.	The transmitter sub-system and the receiver sub-system are collocated in the Accused Instrumentalities.         More specifically, the iPhone is a computing device that includes the transmitter sub-system and the receiver sub-system.
	Tendi Sense Sector MA Data Sense Sector System in other
	Becar bevecters linear The Security Interest Interest composition (Ex. A, Apple Plaform Security, at 9.)

Claim 10	Accused Instrumentalities
10. A transmitter sub- system for operating in a system for providing secure access to a controlled item, wherein the transmitter sub-system comprises:	To the extent that the preamble is deemed to be a limitation, the Accused Instrumentalities are configured to use a system in accordance with this claim.
10a. a biometric sensor configured to receiving a biometric signal;	<ul> <li>The Accused Instrumentalities include a biometric sensor configured to receive a biometric signal.</li> <li>More specifically, the iPhone has at least one biometric sensor for capturing a fingerprint or a face (Touch ID and/or Face ID), namely a Touch ID sensor and a camera system with image sensor, respectively.</li> <li>Touch ID</li> </ul>
	<ul> <li>"Apple devices with a Touch ID sensor can be unlocked using a fingerprint."</li> <li>(Ex. A, Apple Platform Security, at 19.)</li> <li>"Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the sensor continuing to expand the fingerprint map as additional overlapping nodes are identified with each use."</li> <li>(<i>Id.</i>)</li> <li>"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave."</li> <li>(<i>Id.</i>)</li> </ul>

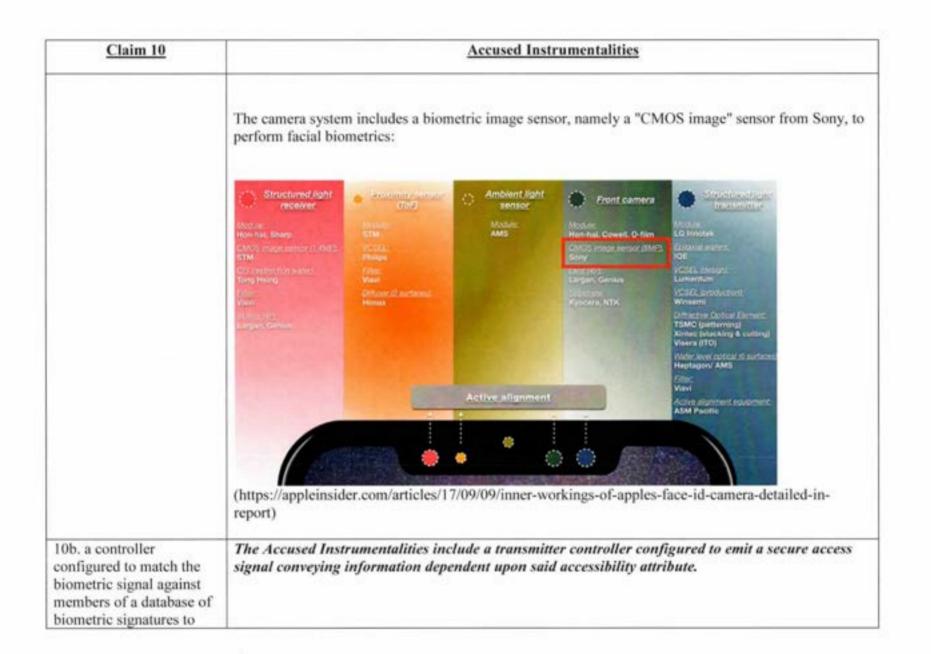
# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 57 of 232

Claim 10	Accused Instrumentalities
	The biometric sensor for Touch ID is located below the home button: "The Home button is a stack of different materials, capped with a sapphire crystal lens. The surrounding stainless-steel ring works as a ground and detects the user's finger. This action activates capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors." (https://appleinsider.com/inside/touch-id) "The Home button is a stack of different materials, capped with a sapphire crystal lens. The surrounding stainless-steel ring works as a ground and detects the user's finger. This action activates capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors." (https://appleinsider.com/inside/touch-id) "Laser-cut sapphire cryst. Sainless steel detection ring Touch ID sensor Touch ID sensor
	Biometric sensor 121 "Where is the Touch ID sensor located? The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top
	button. (https://support.apple.com/en-us/HT201371)
	The image sensor captures an 88-by-88-pixel, 500 PPI raster scan:

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 58 of 232

<u>Claim 10</u>	Accused Instrumentalities
	"The 88-by-88-pixel, 500-ppi raster scan is temporarily stored in encrypted memory within the Secure Enclave while being vectorized for analysis, and then it's discarded. The analysis utilizes subdermal ridge flow angle mapping, which is a lossy process that discards minutia data that would be required to reconstruct the user's actual fingerprint. The resulting map of nodes is stored without any identity information in an encrypted format that can only be read by the Secure Enclave, and is never sent to Apple or backed up to iCloud or iTunes. " (Ex. C, iOS Security white paper, at 8.)
	Face ID
	The biometric sensor for facial biometrics is a camera system ("TrueDepth camera system") with an image sensor.
	"With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face." (Ex. A, Apple Platform Security, at 20.)
	To receive a biometric signal, the camera system with image sensor reads over 30,000 infrared points to capture depth information along with a two-dimensional infrared image.
	"After the TrueDepth camera confirms the presence of an attentive face, it projects and <b>reads over</b> <b>30,000 infrared dots to form a depth map of the face along with a 2D infrared image</b> . This data is used to <b>create a sequence of 2D images and depth maps</b> , which are digitally signed and sent to the Secure Enclave. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." ( <i>Id.</i> )

### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 59 of 232



# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 60 of 232

Claim 10	Accused Instrumentalities
thereby output an accessibility attribute; and	More specifically, the iPhone's System on Chip (SOC), i.e. the Secure Enclave with its Secure Enclave Processor (SEP) or a Secure Neural Engine contained therein, is a means (103) to check a match of the biometric signal with elements of the biometric signature database.
	"The Secure Enclave is a system on chip (SoC) that is included on all recent iPhone, devices" (Ex. A, Apple Platform Security, at 7.)
	"During <b>matching</b> , the Secure Enclave <b>compares</b> incoming data from the biometric sensor against the stored templates <b>to determine whether to unlock the device</b> or respond that a match is valid (for Apple Pay, in-app, and other uses of Touch ID and Face ID). " ( <i>Id.</i> , at 19.)
	The biometric signal received from the biometric sensor ("incoming data from the biometric sensor") is thus checked by the Secure Enclave and its SEP with the elements of the database of biometric signatures 105, i.e. the "stored templates", for the presence of a match.
	For Touch ID, the Secure Enclave match verification is performed as follows:
	"The Secure Enclave is responsible for processing fingerprint data from the Touch ID sensor, determining if there is a match against registered fingerprints, and then enabling access or purchases on behalf of the user" (Ex. C, iOS Security white paper, at 7.)
	"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches" (Ex. A, Apple Platform Security, at 19.)
	"Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. " (https://support.apple.com/en-us/HT204587)

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 61 of 232

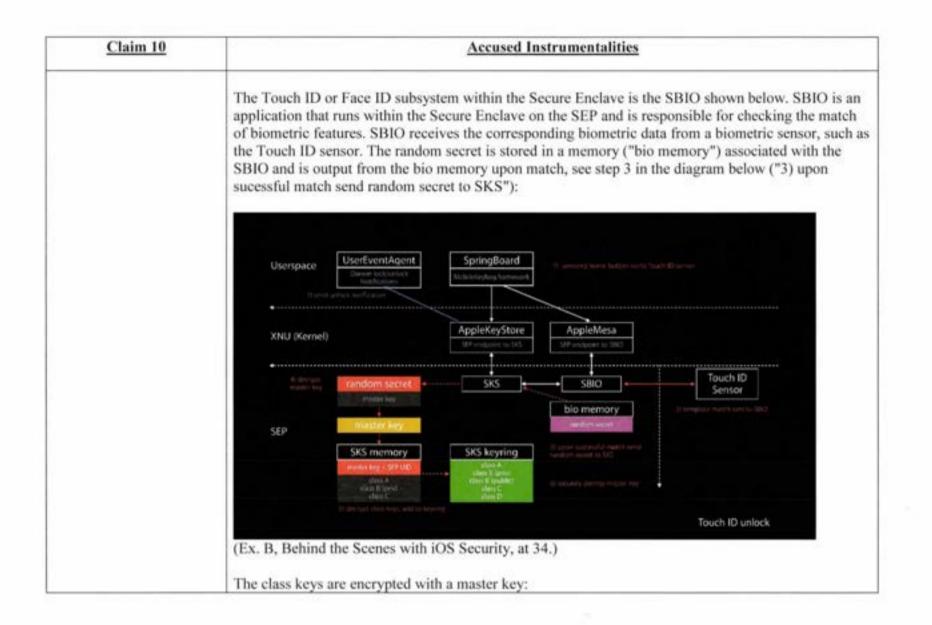
<u>Claim 10</u>	Accused Instrumentalities
	"Touch ID can read multiple fingerprints and recognize fingerprints at any orientation of the finger. The system then creates a mathematical representation of your fingerprint and compares it to the registered fingerprint data to determine a match and unlock your device." (https://support.apple.com/de-de/HT204587)
	For <b>Face ID</b> , the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:
	"Face ID uses neural networks for determining attention, <b>matching</b> , and antispoofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)
	"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." ( <i>Id.</i> ).
	"Facial matching security
	Facial matching is performed within the Secure Enclave using neural networks trained specifically for that purpose Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device." ( <i>Id.</i> at 23.)
	When the Secure Enclave, or more precisely the Touch ID or Face ID subsystem within the Secure Enclave, has determined that a match exists, an accessibility attribute is issued by the corresponding Touch ID or Face ID subsystem. This Touch ID or Face ID subsystem is also referred to as the SBIO. The accessibility attribute confirms that there is a match and that the iPhone is to be unlocked (" determine whether to unlock the device").

ASSA ABLOY Ex. 1021 - Page 60 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 62 of 232

Claim 10	Accused Instrumentalities
	This confirmation of the match is signaled by the SBIO by issuing a random secret to which only the Touch ID or Face ID subsystem within the Secure Enclave has access:
	"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device []." ( <i>Id.</i> at 19.)
	"Uses for Touch ID and Face ID
	Unlocking a device or user account
	[] keys for the highest class of Data Protection-which are held in the Secure Enclave [].
	With Touch ID or Face ID enabled, the keys aren't discarded when the device or account locks; instead, they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the Secure Enclave. When a user attempts to unlock the device or account, if the device detects a successful match, it provides the key for unwrapping the Data Protection keys, and the device or account is unlocked. This process provides additional protection by requiring cooperation between the Data Protection and Touch ID or Face ID subsystems to unlock the device."
	( <i>Id.</i> at 24.)
	"The class key is protected with the hardware UID and, for some classes, the user's passcode." ( <i>Id.</i> at 85.)
	"Complete Protection
	<i>(NSFileProtectionComplete):</i> The class key is protected with a key derived from the user passcode or password and the device UID. Shortly after the user locks a device (10 seconds, if the Require Password setting is Immediately), the decrypted class key is discarded, rendering all data in this class inaccessible until the user enters the passcode again or unlocks (logs in to) the device using Touch ID or Face ID."
	( <i>Id.</i> at 86.)

### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 63 of 232



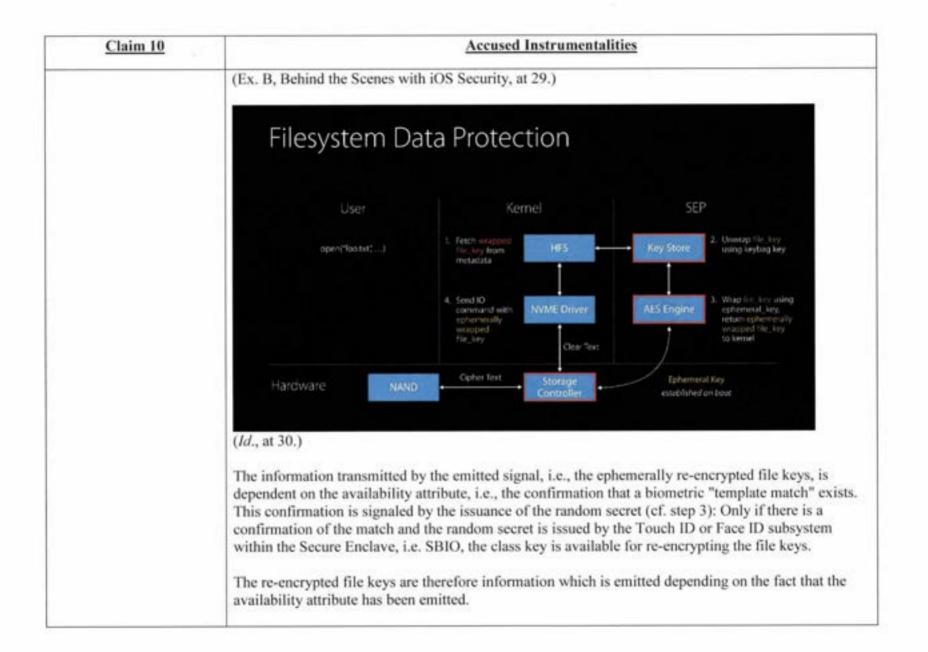
ASSA ABLOY Ex. 1021 - Page 62 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

Claim 10	Accused Instrumentalities
	User Keybags
	Background
	Sets of keys generated for each user to protect their data at rest
	Keys wrapped by master key derived from user passcode and SEP UID
	After 10 incorrect passcode entries, SEP will not process any further attempts
	Different policy associated with each keybag key—Usage, availability
	( <i>Id.</i> , at 25.)
	The random secret is issued to SKS. SKS is a Secure Key Service application which is located within the Secure Enclave on the SEP and is responsible for decrypting class keys. The random secret provided by SBIO is used to decrypt a master key ("4) decrypt master key"). The master key is concatenated with the UID of the SEP and thus class keys are decrypted and added to the SKS keyring ("5) decrypt class keys, add to keyring") for further use by the Secure Enclave. The decrypted class keys include, for example, the class key of class A.
10c. a transmitter configured to emit a secure access signal	The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.
conveying said information dependent	For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys:
upon said accessibility attribute;	"sepOS can then use the ephemeral wrapping key to wrap file keys for use by the Application Processor file-system driver. When the file-system driver reads or writes a file, it sends the wrapped key to the AES Engine."

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 65 of 232

Claim 10	Accused Instrumentalities
	(Ex. A, Apple Platform Security, at 14.)
	"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. [] When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." ( <i>Id.</i> at 85.)
	The signal with the ephemerally re-encrypted file keys is a secure signal because it comes from the Secure Enclave and thus from a secure environment. Furthermore, the signal is secure because the transmitted information is encrypted. The emitted file keys are encrypted with the ephemeral key:
	"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. At startup, the Secure Enclave negotiates an ephemeral key with the AES Engine. When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." ( <i>Id.</i> )
	Filesystem Data Protection
	Overview
	File blocks are encrypted using AES-XTS with 128-bit keys
	Each file on the user partition is encrypted using a unique random key chosen by SE
	Raw file keys are never exposed to the AP
	Wrapped with a key from the user keybag for long-term storage
	<ul> <li>Wrapped with an ephemeral key while in use, bound to boot session</li> </ul>

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 66 of 232



<u>Claim 10</u>	Accused Instrumentalities
10d. wherein the controller is further configured to:	The Accused Instrumentalities include a controller that is configured to be used as set forth in elements 10d1, 10d2, and 10d3 below.
10d1. receive a series of entries of the biometric signal, said series being	The Accused Instrumentalities include a transmitter sub-system controller configured to receive a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry.
characterised according to at least one of the number of said entries and a duration of each said	More specifically, the Secure Enclave of the iPhone with the Secure Enclave Processor forms the means for receiving a series of entries of the biometric signal.
entry;	"Apple's biometric security architecture relies on a strict separation of responsibilities between the biometric sensor and the Secure Enclave, and a secure connection between the two. The sensor captures the biometric image and securely transmits it to the Secure Enclave." (Ex. A, Apple Platform Security, at 19.)
	Touch ID
	When a finger is placed on the biometric sensor, the finger is scanned and the corresponding biometric signal entry is received by the Secure Enclave.
	"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave." ( <i>Id.</i> )
	To enroll a fingerprint in the database, the iPhone's fingerprint sensor records an entry of a biometric signal when the user places his finger on the sensor. This is done multiple times, resulting in a series of entries of such biometric signals.
	Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone.

<u>Claim 10</u>	Accused Instrumentalities
	Set up Touch ID
	<ul> <li>Before you can set up Touch ID, you must first create a <u>code</u> for your device,* then follow these steps:</li> <li>7. Make sure the Touch ID sensor and your finger are clean and dry.</li> </ul>
	8. Tap Settings > Touch ID & Code, and then enter your code.
	<ol><li>Tap "Add fingerprint" and hold the device as you normally would when touching the Touch ID sensor.</li></ol>
	10. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.
	Ind the set of the set
	11. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 69 of 232

Claim 10	Accused Instrumentalities
	12. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you would during the first scan."
	(https://support.apple.com/en-us/HT201371)
	Accordingly, the user is prompted to place his finger on the sensor several times, in particular in accordance with step 5. Each time the finger is placed on the sensor, a corresponding biometric entry is generated, i.e. a series of such entries. All these entries, which result from placing the same finger on the sensor, form a series.
	Face ID
	The means for receiving a series of entries of the biometric signal includes a Secure Neural Engine, which is protected by the Secure Enclave. The Secure Neural Engine transforms the series of entries of the biometric signal received by the Secure Enclave into a biometric signature ("mathematical representation").
	"After the TrueDepth camera confirms the presence of an attentive face, it projects and reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image. This data is used to create <b>a sequence of 2D images and depth maps</b> , which are digitally signed and <b>sent to the Secure Enclave</b> . To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)
	Each entry of the biometric signal thus contains a two-dimensional infrared image with 30,000 infrared points for capturing depth information. By continuously capturing such infrared images into a Face ID scan while the user moves his head into different poses, a series of entries of the biometric signal

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 70 of 232

<u>Claim 10</u>	Accused Instrumentalities
	results. Two such Face ID scans are required to generate a biometric signature of a single face, so that two series of entries of the biometric signal are received accordingly.
	Using Face ID on iPhone
	1. Tap Settings > Face ID & Code. Enter your code when prompted.
	2. Tap on "Configure Face ID".
	3. Hold the device in portrait mode in front of your face and tap "Let's go".
	4. Make sure your face is inside the frame and slowly move your head until the circle shown is completed. If you can't move your head, tap on "Options for operating aids".
	5. After performing the first Face ID scan, tap "Next".
	6. Again, slowly describe a circle with your head until it is completed.
	7. Tap "Done."
	(https://support.apple.com/en-us/HT208109)
	The biometric signature of a single face is thus determined by two successive Face ID scans, each of which receives a series of entries of the biometric signal (compare steps 4. and 6. above).
	To register a second face, the iPhone offers a corresponding option in its settings. If the user selects the option "Set up an alternative appearance" as shown in the figure below on https://www.macworld.co.uk/how-to/second-face-id-3803421/, a second face is registered by the iPhone in the same way as the first face.

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 71 of 232

Claim 10	Accused Instrumentalities
	Camatanan Face ID & Passcode
	10.2
	LOD FACE ID FOR
	Phone Unlock
	iTure App Store
	Assi
	Pasawo utofil
	Other Add 4 Again 1-
	Attende Lader 1. And de Alagaire. Minner conservational Rectaures of an anti-anti-anti-anti-anti-anti-anti-anti-
	Set Up an Alternative Appearance
	lei astillitar ko senetinastaluk hainneg hum joss taan, Fann 10 curi moogrida an alternatist appearance.
	Result Face (D
	Account Attention for Face ID
	The series of entries of the biometric signal is identified on the iPhone by both the number and duration of each such entry.
	Touch ID
	According to step 5 of the instructions https://support.apple.com/en-us/HT201371, for the enrollment of a single finger, the user has to repeatedly place the respective finger on the sensor and thus a number of entries in a row predetermined via the user guidance are captured by the iPhone. Each one of the entries must also be of a predetermined duration given to the user via the iPhone directory is a the user's sensor.
	entries must also be of a predetermined duration given to the user via the iPhone display, i.e. the user's finger must remain on the sensor for a predetermined duration for each entry of the biometric signal in order to capture the biometric signal during this time.

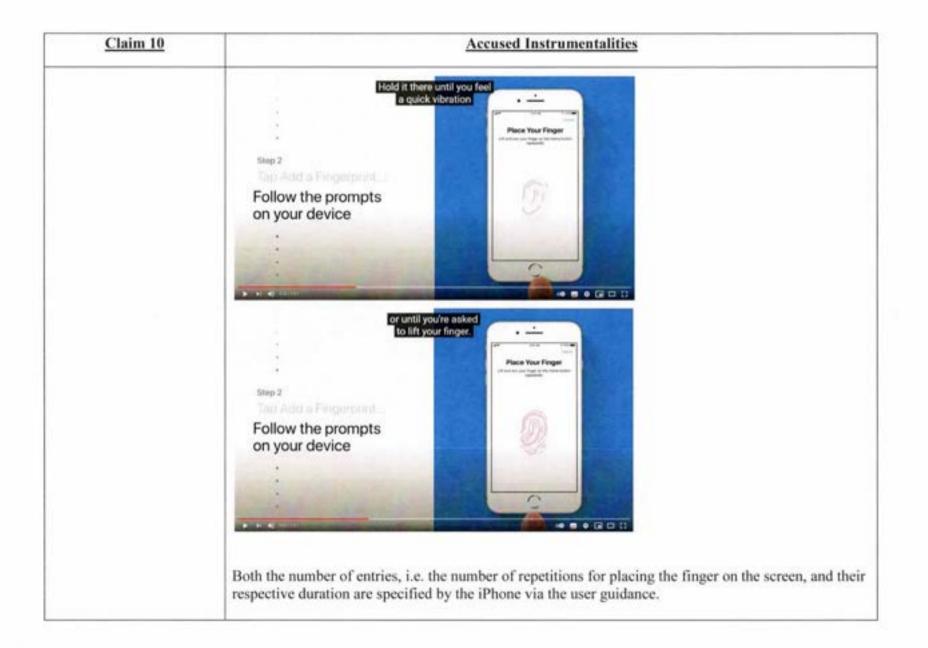
# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 72 of 232

Claim 10	Accused Instrumentalities
	Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone and iPad.
	Set up Touch ID
	<ul> <li>4. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</li> </ul>
	-at ♦ • 41 km C.ur.us C.ur.us
	Place Your Finger Lift and rest your friger on the Home button repeatedly.
	5. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.
	6. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you did during the first scan.
	(https://support.apple.com/en-us/HT201371)

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 73 of 232

Claim 10	Accused Instrumentalities
	After placing a finger on the home button, a fingerprint appears on the display with red progress bars spreading along some of the papillary bars until the capture of the biometric entry in question is complete:
	When the required duration is reached, the iPhone vibrates after an entry of the biometric signal is received or it issues a prompt to the user to lift the finger. The user then lifts the finger in question and replaces the same finger so that the iPhone receives a series of biometric signal entries of sufficient duration for that finger. The process is repeated for the same finger for as long as required according to the iPhone's user guidance. This is shown in the Apple You Tube video (32) How to set up Touch ID on your iPhone or iPad - Apple Support - YouTube (https://www.youtube.com/watch?v=xTZ2LALWZlg):

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 74 of 232



# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 75 of 232

Claim 10	Accused Instrumentalities
	Face ID The user moves his face in front of the camera to strike different poses, and the camera system with image sensor continuously captures a large number of biometric entries, i.e. here the 2D images with depth information, in a row.
	"This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)
	The sufficient duration of an entry for a pose, i.e. an angular position of the head specified via the user interface of the iPhone, is indicated to the user by the transformation of a gray line into a green line:
	More proof fixed structly fix complete the details     More proof fixed structly fix complete the details     More proof fixed structly fix complete the details     Fault Face 45 state
0.12 man mid and a late	(Individual images taken from: https://support.apple.com/en-us/HT208109)
0d2. map said series into n instruction; and	The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 76 of 232

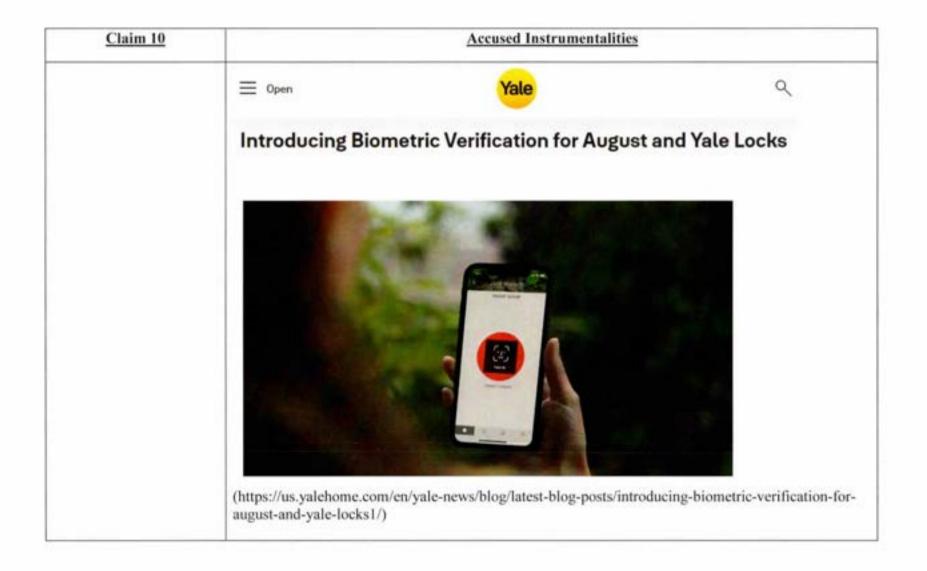
<u>Claim 10</u>	Accused Instrumentalities
	More specifically, the Secure Enclave of the iPhone contains means to assign the received row to an instruction: The Secure Enclave, after receiving the full set of entries of the biometric signal, assigns this set to an instruction for processing, encrypting and storing the biometric signature ("Touch ID and Face ID template data").
	"The sensor captures the biometric image and securely transmits it to the Secure Enclave. During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Ex. A, Apple Platform Security, at 19.)
	To carry out this instruction, the Secure Enclave has its own processor: "The Secure Enclave Processor provides the main computing power for the Secure Enclave." ( <i>Id.</i> , at 10.)
	Touch ID
	The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.
	"The analysis uses subdermal ridge flow angle mapping, a lossy process that discards "finger minutiae data" that would be required to reconstruct the user's actual fingerprint. During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches, but without any identity information." ( <i>Id.</i> , at 19.)
	<b>Face ID</b> The instruction involves the transformation of the set of entries of the biometric signal captured via the Face ID scans into a mathematical representation, i.e. the biometric signature of the face in question by the Secure Neural Engine of the Secure Enclave, as well as its encryption and storage.

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 77 of 232

<u>Claim 10</u>	Accused Instrumentalities
	"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses. " ( <i>Id.</i> , at 20.)
	"Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device. It's not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:
	<ul> <li>The mathematical representations of a user's face calculated during enrollment</li> <li>"</li> </ul>
	( <i>Id.</i> , at 23.)
10d3. populate the database according to the instruction, wherein the	The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.
controlled item is one of: a locking mechanism of a physical access structure	More specifically, the Secure Enclave stores the biometric signature, i.e. the encrypted mathematical representation of the fingerprint or face, in the database 105, i.e. the "secure nonvolatile storage":
or an electronic lock on an electronic computing device.	"The secure nonvolatile storage is used for all anti-replay services in the Secure Enclave. Anti-replay services on the Secure Enclave are used for revocation of data over events that mark anti-replay boundaries including, but not limited to, the following:
	<ul> <li></li> <li>Adding or removing a Touch ID fingerprint or Face ID face".</li> <li>(Ex. A, Apple Platform Security, at 16.)</li> </ul>
	"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." ( <i>Id.</i> , at 19.)

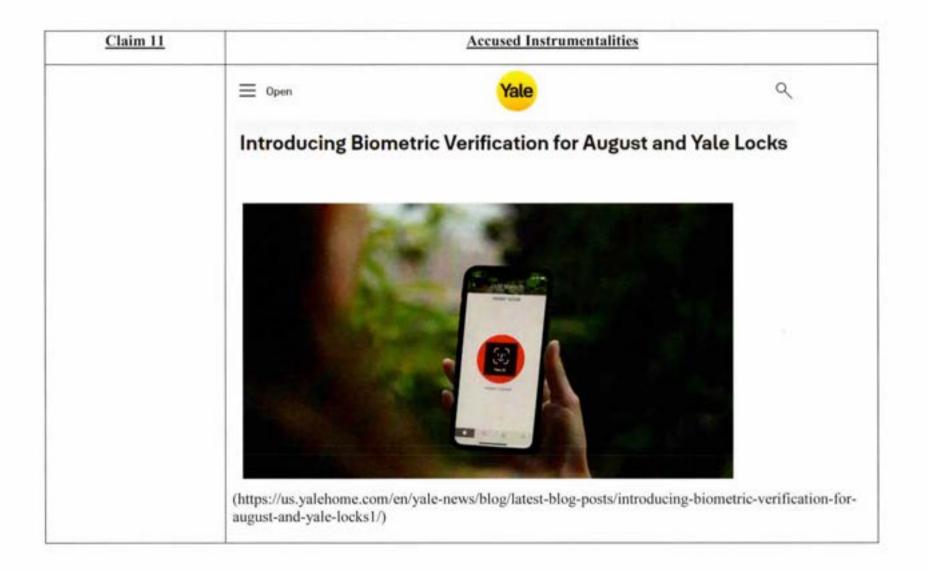
# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 78 of 232

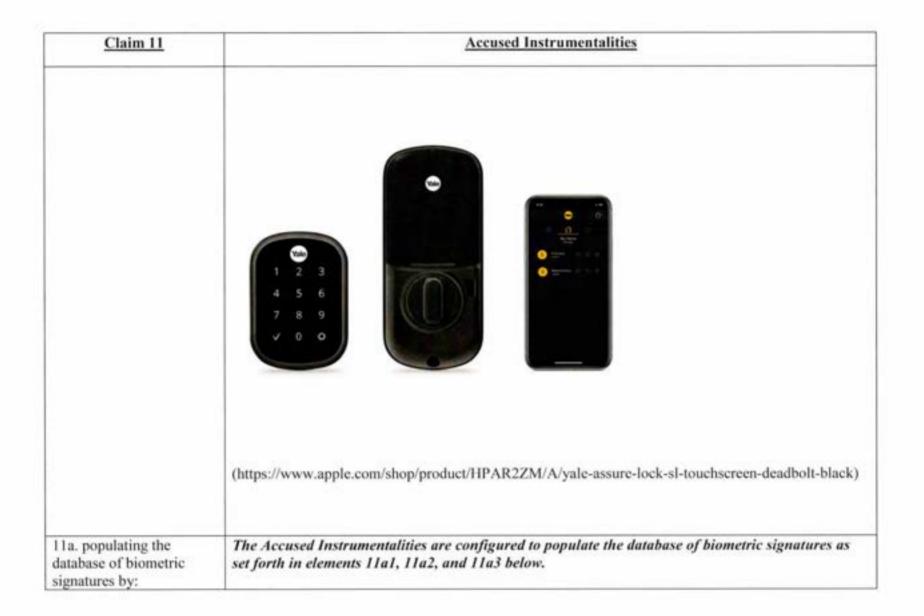
Claim 10	Accused Instrumentalities
	Touch ID
	"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches" ( <i>Id.</i> )
	Face ID
	The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:
	The mathematical representations of a user's face calculated during enrollment".     ( <i>Id.</i> , at 23.)
	More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.
	"When the "Secure Remote Access" feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it."
	<pre>(https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for- august-and-yale-locks1/)</pre>





Accused Instrumentalities
Accused Instrumentalities  t that the preamble is deemed to be a limitation, the Accused Instrumentalities are o use a method in accordance with this claim.  cally, the controlled item is a locking mechanism of the door lock of the user's home. The rumentalities are configured to provide secure access to the user's home via Yale Smart the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face Secure Remote Access'' feature is turned on, the app will use your phone's built-in n tools to prompt fingerprint or facial recognition before you can unlock or lock your dy (note: if your phone does not have these features, it will prompt you to use your PIN urther ensures that your door is only operated by the right people at the time you intend lehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for- ale-locks1/)





## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 84 of 232

Claim 11	Accused Instrumentalities
11a1. receiving a series of entries of the biometric signal;	The Accused Instrumentalities are configured to populate the database of biometric signatures by: receiving a series of entries of the biometric signal.
	More specifically, the Secure Enclave of the iPhone with the Secure Enclave Processor forms the means for receiving a series of entries of the biometric signal.
	"Apple's biometric security architecture relies on a strict separation of responsibilities between the biometric sensor and the Secure Enclave, and a secure connection between the two. The sensor captures the biometric image and securely transmits it to the Secure Enclave." (Ex. A, Apple Platform Security, at 19.)
	Touch ID
	When a finger is placed on the biometric sensor, the finger is scanned and the corresponding biometric signal entry is received by the Secure Enclave.
	"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave." (Ex. A, Apple Platform Security, at 19.)
	To enroll a fingerprint in the database, the iPhone's fingerprint sensor records an entry of a biometric signal when the user places his finger on the sensor. This is done multiple times, resulting in a series of entries of such biometric signals.
	Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone.
	Set up Touch ID
	Before you can set up Touch ID, you must first create a <u>code</u> for your device,* then follow these steps: 1. Make sure the Touch ID sensor and your finger are clean and dry.

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 85 of 232

<u>Claim 11</u>	Accused Instrumentalities
	2. Tap Settings > Touch ID & Code, and then enter your code.
	3. Tap "Add fingerprint" and hold the device as you normally would when touching the Touch ID sensor.
	<ul> <li>4. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</li> <li>Place Your Finger Ut and maximum press of the torne button inpress of the torne button in the torne</li></ul>
	<ul><li>5. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.</li></ul>
	6. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you would during the first scan."
	(https://support.apple.com/en-us/HT201371)

<u>Claim 11</u>	Accused Instrumentalities
	Accordingly, the user is prompted to place his finger on the sensor several times, in particular in accordance with step 5. Each time the finger is placed on the sensor, a corresponding biometric entry is generated, i.e. a series of such entries. All these entries, which result from placing the same finger on the sensor, form a series.
	Face ID
	The means for receiving a series of entries of the biometric signal includes a Secure Neural Engine, which is protected by the Secure Enclave. The Secure Neural Engine transforms the series of entries of the biometric signal received by the Secure Enclave into a biometric signature ("mathematical representation").
	"After the TrueDepth camera confirms the presence of an attentive face, it projects and reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image. This data is used to create <b>a sequence of 2D images and depth maps</b> , which are digitally signed and <b>sent to the Secure Enclave</b> . To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the <b>Secure Neural Engine-protected</b> within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (emphasis added) (Ex. A, Apple Platform Security, at 20.)
	Each entry of the biometric signal thus contains a two-dimensional infrared image with 30,000 infrared points for capturing depth information. By continuously capturing such infrared images into a Face ID scan while the user moves his head into different poses, a series of entries of the biometric signal results. Two such Face ID scans are required to generate a biometric signature of a single face, so that two series of entries of the biometric signal are received accordingly.
	Using Face ID on iPhone or iPad Pro - Apple Support

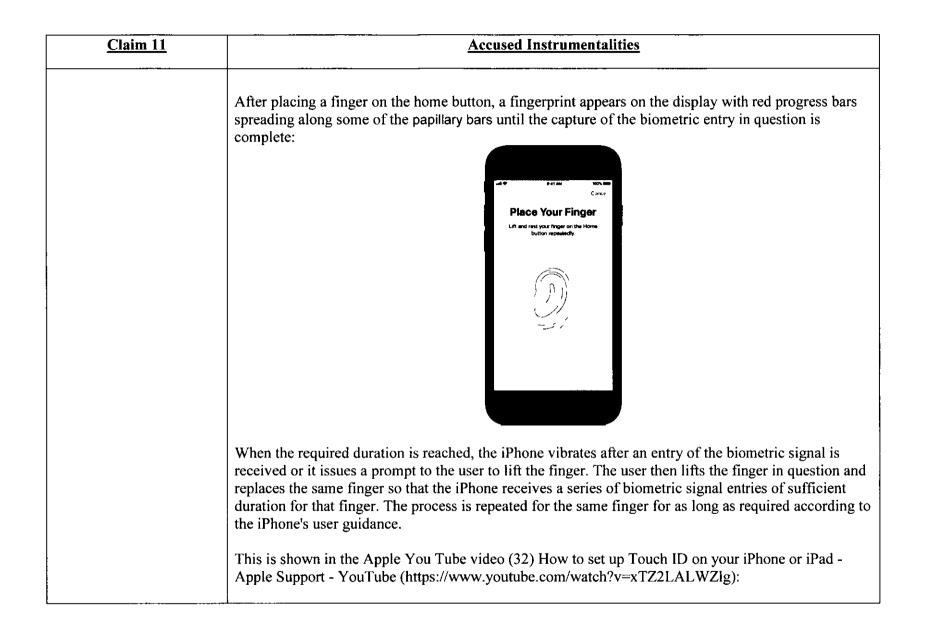
# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 87 of 232

<u>Claim 11</u>	Accused Instrumentalities
	Configure Face ID
	Before configuring Face ID, make sure that neither the TrueDepth camera nor your face are covered by anything
	Follow the steps below to configure Face ID:
	1. Tap Settings > Face ID & Code. Enter your code when prompted.
	2. Tap on "Configure Face ID".
	3. Hold the device in portrait mode in front of your face and tap "Let's go".
	4. Make sure your face is inside the frame and slowly move your head until the circle shown is completed. If you can't move your head, tap on "Options for operating aids".
	5. After performing the first Face ID scan, tap "Next".
	6. Again, slowly describe a circle with your head until it is completed.
	7. Tap "Done."
	(https://support.apple.com/en-us/HT208109)
	The biometric signature of a single face is thus determined by two successive Face ID scans, each of which receives a series of entries of the biometric signal (compare steps 4. and 6. above).
	To register a second face, the iPhone offers a corresponding option in its settings. If the user selects the option "Set up an alternative appearance" as shown in the figure below on https://www.macworld.co.uk/how-to/second-face-id-3803421/, a second face is registered by the iPhone in the same way as the first face.

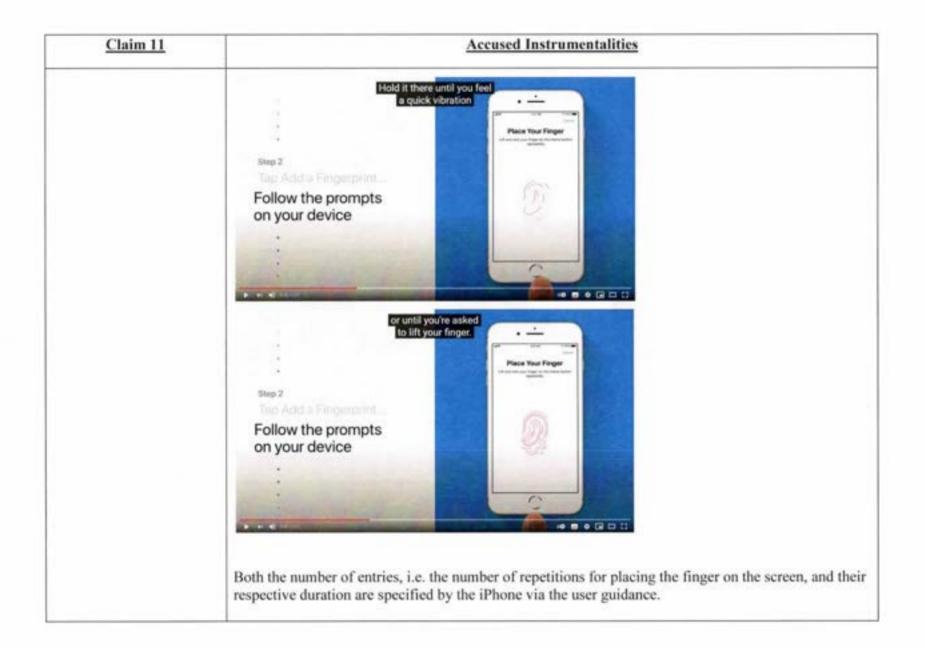
#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 88 of 232

Claim 11	Accused Instrumentalities
	Cartilisas Face ID & Passcode
	15.2
	[w]
	Late Nece to the
	Phone Unlack
	iTure App Store
	Acciv
	Passes LtoFil
	Other Apt 4 Apt 4
	Proved part A and the first compare types dimensional features of a second sec
	Set Up an Alternative Appearation
	let antifitiare to constituancely learning from provintion, finite 10 cars - sectoryment an internative approximation.
	Reset Face ID
	ATTUNION
	Require Attention for Face ID
	The series of entries of the biometric signal is identified on the iPhone by both the number and
	duration of each such entry.
	Touch ID
	According to step 5 of the instructions https://support.apple.com/en-us/HT201371, for the enrollment
	of a single finger, the user has to repeatedly place the respective finger on the sensor and thus a number
	of entries in a row predetermined via the user guidance are captured by the iPhone. Each one of the
	entries must also be of a predetermined duration given to the user via the iPhone display, i.e. the user's
	finger must remain on the sensor for a predetermined duration for each entry of the biometric signal in
	order to capture the biometric signal during this time.

<u>Claim 11</u>	Accused Instrumentalities
	Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone.
	Set up Touch ID
	4. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.
	ил Ф. Виллан зорушен Сапчо-
	Place Your Finger Lift and rest your finger on the Home
	button repeatedly.
	5. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.
	<ul> <li>6. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you did during the first scan.</li> </ul>
	(https://support.apple.com/en-us/HT201371)



#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 91 of 232



# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 92 of 232

Claim 11	Accused Instrumentalities
	Face ID
	The user moves his face in front of the camera to strike different poses, and the camera system with image sensor continuously captures a large number of biometric entries, i.e. here the 2D images with depth information, in a row.
	"This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)
	The sufficient duration of an entry for a pose, i.e. an angular position of the head specified via the use interface of the iPhone, is indicated to the user by the transformation of a gray line into a green line:
	Move your freed streety to complete the circle. First Face D scale complete the circle.
	(Individual images taken from: https://support.apple.com/en-us/HT208109)

<u>Claim 11</u>	Accused Instrumentalities
11a2. determining at least one of the number of said entries and a duration of	The Accused instrumentalities are configured to populate the database of biometric signatures by: determining at least one of the number of said entries and a duration of each said entry.
each said entry;	More specifically, as discussed above, both Face ID and Touch ID require a specific number of entries to enroll a Touch ID or Face ID. The Accused Instrumentalities must determine that the specific number of entries have been input. Likewise, while not necessary for the claim, upon information and belief, the Accused Instrumentalities determine that each input of either facial or fingerprint data is of a sufficient duration. Again, when setting up Touch ID in the Accused Instrumentalities, the users are required to touch the home button with their finger several times for a certain duration. Similarly, the users need to scan their face twice, and each scan requires the users to move their head in a circle for a certain duration for Face ID.
	Touch ID: Register a fingerprint for Apple Touch ID by the user tapping a finger several times on the home button to record the fingerprint data. (https://video.search.yahoo.com/yhs/search?fr=yhs-pty_pty_ converter&hsimp=yhs- pty_converter&hspart=pty&p=registering+ fingerprint+apple+touch+id+on+screen+instructions#id=1&vid= 156de65ae06ca453643009fc0ea9cf79&action=click)
	Touch ID: The user's finger must remain on the home button long enough for the data to be recorded. "Touch the Touch ID sensor with your finger, but don't press it. Hold it there until you feel a quick vibration, or until you're asked to lift your finger." "Continue to lift and rest your finger slowly, making small adjustments to the position of your finger each time." (https://support.apple.com/en-au/HT201371)
	Touch ID: "you shouldn't tap too quickly or move your finger around" (https://support.apple.com/en-us/HT207537)
	Face ID: Setting up Face ID requires two scans of the user's face. Each scan asks users to move their head slowly in a circle to register different angles of the user's face. (https://www.imore.com/how-set-face-id-iphone)

<u>Claim 11</u>	Accused Instrumentalities
11a3. mapping said series into an instruction; and	The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.
	More specifically, the Secure Enclave of the iPhone contains means to assign the received row to an instruction: The Secure Enclave, after receiving the full set of entries of the biometric signal, assigns this set to an instruction for processing, encrypting and storing the biometric signature ("Touch ID and Face ID template data").
	"The sensor captures the biometric image and securely transmits it to the Secure Enclave. During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Ex. A, Apple Platform Security, at 19.)
	To carry out this instruction, the Secure Enclave has its own processor: "The Secure Enclave Processor provides the main computing power for the Secure Enclave." ( <i>Id.</i> , at 10.)
	Touch ID
	The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.
	"The analysis uses subdermal ridge flow angle mapping, a lossy process that discards "finger minutiae data" that would be required to reconstruct the user's actual fingerprint. During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches, but without any identity information." ( <i>Id.</i> , at 19.)
	Face ID

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 95 of 232

<u>Claim 11</u>	Accused Instrumentalities
	The instruction involves the transformation of the set of entries of the biometric signal captured via the Face ID scans into a mathematical representation, i.e. the biometric signature of the face in question by the Secure Neural Engine of the Secure Enclave, as well as its encryption and storage.
	"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses. " ( <i>Id.</i> , at 20.)
	<ul> <li>"Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device. It's not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:</li> <li>The mathematical representations of a user's face calculated during enrollment</li> </ul>
	•" ( <i>Id.</i> , at 23.)
1 1a4. populating the database according to the instruction;	The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.
	More specifically, the Secure Enclave stores the biometric signature, i.e. the encrypted mathematical representation of the fingerprint or face, in the database 105, i.e. the "secure nonvolatile storage":
	"The secure nonvolatile storage is used for all anti-replay services in the Secure Enclave. Anti-replay services on the Secure Enclave are used for revocation of data over events that mark anti-replay boundaries including, but not limited to, the following:
	•
	<ul> <li>Adding or removing a Touch ID fingerprint or Face ID face".</li> <li>(Ex. A, Apple Platform Security, at 16.)</li> </ul>

<u>Claim 11</u>	Accused Instrumentalities
	"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." ( <i>Id.</i> , at 19.)
	Touch ID
	"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches" ( <i>Id.</i> )
	Face ID
	The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:
	• The mathematical representations of a user's face calculated during enrollment". ( <i>Id.</i> , at 23.)
11b. receiving the biometric signal;	The Accused Instrumentalities include a biometric sensor configured to receive the biometric signal.
	More specifically, the iPhone has at least one biometric sensor for capturing a fingerprint or a face (Touch ID and/or Face ID), namely a Touch ID sensor and a camera system with image sensor, respectively.
	Touch ID
	"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.)
	"Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the <b>sensor</b> continuing to expand the fingerprint map as additional overlapping nodes are identified with each use."

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 97 of 232

<u>Claim 11</u>	Accused Instrumentalities
	<ul> <li>(Id.)</li> <li>"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave."</li> <li>(Id.)</li> </ul>
	The biometric sensor for Touch ID is located below the home button: "The Home button is a stack of different materials, capped with a sapphire crystal lens. The surrounding stainless-steel ring works as a ground and detects the user's finger. This action activates a capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors." (https://appleinsider.com/inside/touch-id)
	Laser-cut sapphire cryst
	Stainless steel detection ring Touch ID sensor Tactile switch
	Biometric sensor 121 "Where is the Touch ID sensor located?

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 98 of 232

<u>Claim 11</u>	Accused Instrumentalities
	The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.
	(https://support.apple.com/en-us/HT201371)
	The image sensor captures an 88-by-88-pixel, 500 PPI raster scan:
	"The 88-by-88-pixel, 500-ppi raster scan is temporarily stored in encrypted memory within the Secure Enclave while being vectorized for analysis, and then it's discarded. The analysis utilizes subdermal ridge flow angle mapping, which is a lossy process that discards minutia data that would be required to reconstruct the user's actual fingerprint. The resulting map of nodes is stored without any identity information in an encrypted format that can only be read by the Secure Enclave, and is never sent to Apple or backed up to iCloud or iTunes." (Ex. C, iOS Security white paper, at 8.)
	Face ID
	The biometric sensor for facial biometrics is a camera system ("TrueDepth camera system") with an image sensor.
	"With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face." (Ex. A, Apple Platform Security, at 20.)
	To receive a biometric signal, the camera system with image sensor reads over 30,000 infrared points to capture depth information along with a two-dimensional infrared image.
	"After the TrueDepth camera confirms the presence of an attentive face, it projects and <b>reads over</b> 30,000 infrared dots to form a depth map of the face along with a 2D infrared image. This data is

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 99 of 232

Claim 11	Accused Instrumentalities
	used to create a sequence of 2D images and depth maps, which are digitally signed and sent to Secure Enclave. To counter both digital and physical spoofs, the TrueDepth camera randomizes to sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into mathematical representation and compares that representation to the enrolled facial data. This enr facial data is itself a mathematical representation of the user's face captured across a variety of po ( <i>Id.</i> , at 20.)
	Structured light
	Active alignment Active
	(https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in report)

ASSA ABLOY Ex. 1021 - Page 98 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

<u>Claim 11</u>	Accused Instrumentalities
11c. matching the biometric signal against members of the database	The Accused Instrumentalities include a transmitter controller configured to emit a secure access signal conveying information dependent upon said accessibility attribute.
of biometric signatures to thereby output an accessibility attribute;	More specifically, the iPhone's System on Chip (SOC), i.e. the Secure Enclave with its Secure Enclave Processor (SEP) or a Secure Neural Engine contained therein, is a means (103) to check a match of the biometric signal with elements of the biometric signature database.
	"The Secure Enclave is a system on chip (SoC) that is included on all recent iPhone, devices" (Ex. A, Apple Platform Security, at 7.)
	"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device or respond that a match is valid (for Apple Pay, in-app, and other uses of Touch ID and Face ID). " ( <i>Id.</i> , at 19.)
	The biometric signal received from the biometric sensor ("incoming data from the biometric sensor") is thus checked by the Secure Enclave and its SEP with the elements of the database of biometric signatures 105, i.e. the "stored templates", for the presence of a match.
	For Touch ID, the Secure Enclave match verification is performed as follows:
	"The Secure Enclave is responsible for processing fingerprint data from the Touch ID sensor, determining if there is a match against registered fingerprints, and then enabling access or purchases on behalf of the user" (Ex. C, iOS Security white paper, at 7.)
	"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches" (Ex. A, Apple Platform Security, at 19.)

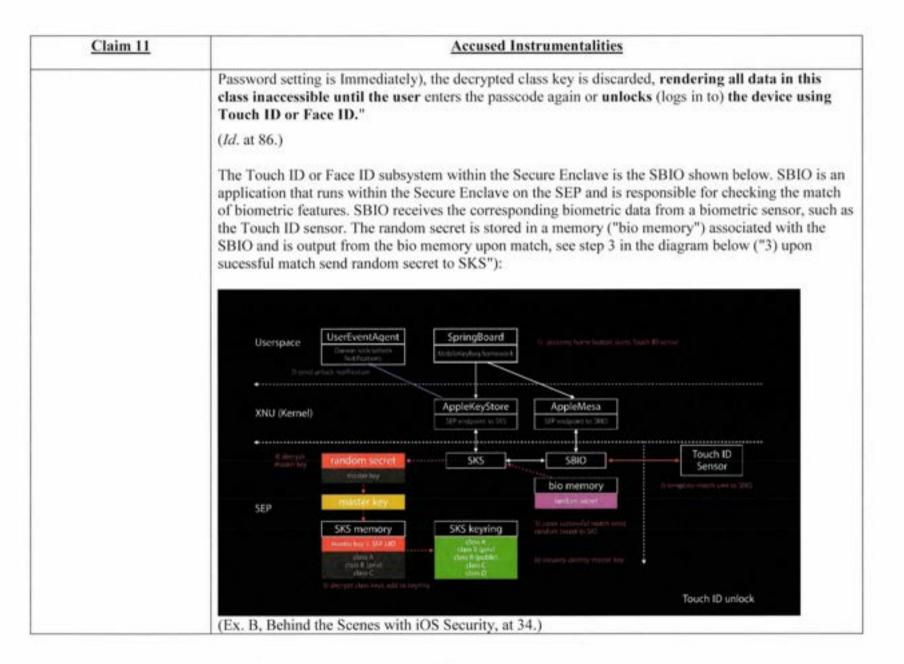
## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 101 of 232

Claim 11	Accused Instrumentalities
	"Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. " (https://support.apple.com/en-us/HT204587)
	"Touch ID can read multiple fingerprints and recognize fingerprints at any orientation of the finger. The system then creates a mathematical representation of your fingerprint and compares it to the registered fingerprint data to determine a match and unlock your device." (https://support.apple.com/de-de/HT204587)
	For <b>Face ID</b> , the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:
	"Face ID uses neural networks for determining attention, <b>matching</b> , and antispoofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)
	"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." ( <i>Id.</i> ).
	"Facial matching security
	Facial matching is performed within the Secure Enclave using neural networks trained specifically for that purpose Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device." ( <i>Id.</i> at 23.)
	When the Secure Enclave, or more precisely the Touch ID or Face ID subsystem within the Secure Enclave, has determined that a match exists, an accessibility attribute is issued by the corresponding

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 102 of 232

Claim 11	Accused Instrumentalities
	Touch ID or Face ID subsystem. This Touch ID or Face ID subsystem is also referred to as the SBIO. The accessibility attribute confirms that there is a match and that the iPhone is to be unlocked (" determine whether to unlock the device").
	This confirmation of the match is signaled by the SBIO by issuing a random secret to which only the Touch ID or Face ID subsystem within the Secure Enclave has access:
	"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device []." ( <i>Id.</i> at 19.)
	"Uses for Touch ID and Face ID
	Unlocking a device or user account
	[] keys for the highest class of Data Protection-which are held in the Secure Enclave [].
	With Touch ID or Face ID enabled, the keys aren't discarded when the device or account locks; instead, they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the Secure Enclave. When a user attempts to unlock the device or account, if the device detects a successful match, it provides the key for unwrapping the Data Protection keys, and the device or account is unlocked. This process provides additional protection by requiring cooperation between the Data Protection and Touch ID or Face ID subsystems to unlock the device."
	( <i>Id.</i> at 24.)
	"The class key is protected with the hardware UID and, for some classes, the user's passcode." ( <i>Id.</i> at 85.)
	"Complete Protection
	(NSFileProtectionComplete): The class key is protected with a key derived from the user passcode or password and the device UID. Shortly after the user locks a device (10 seconds, if the Require

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 103 of 232

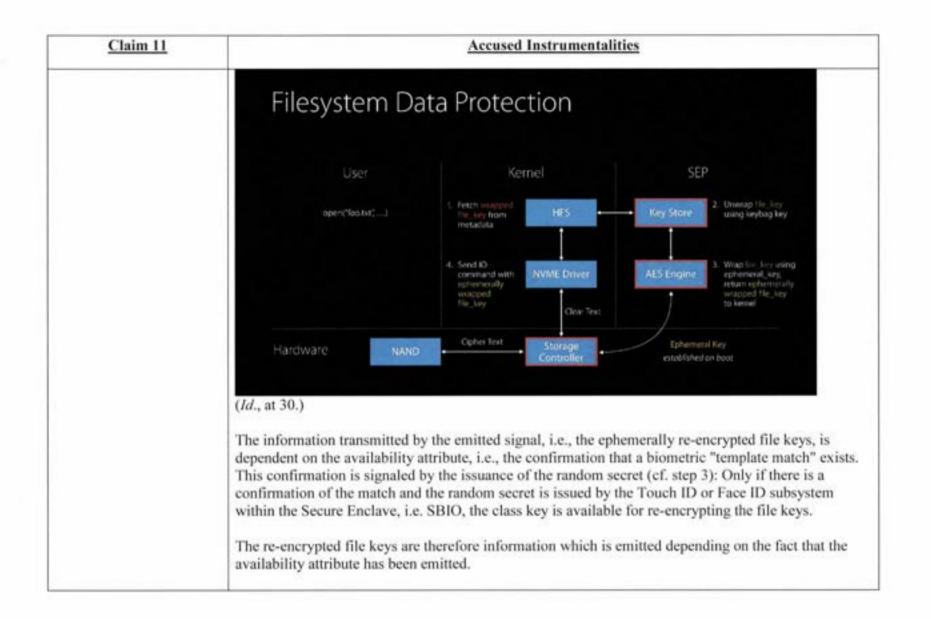


<u>Claim 11</u>	Accused Instrumentalities
	The class keys are encrypted with a master key:
	User Keybags
	Background
	Sets of keys generated for each user to protect their data at rest
	Keys wrapped by master key derived from user passcode and SEP UID
	After 10 incorrect passcode entries, SEP will not process any further attempts
	Different policy associated with each keybag key—Usage, availability
	( <i>Id.</i> , at 25.)
	The random secret is issued to SKS. SKS is a Secure Key Service application which is located within the Secure Enclave on the SEP and is responsible for decrypting class keys. The random secret provided by SBIO is used to decrypt a master key ("4) decrypt master key"). The master key is concatenated with the UID of the SEP and thus class keys are decrypted and added to the SKS keyring ("5) decrypt class keys, add to keyring") for further use by the Secure Enclave. The decrypted class keys include, for example, the class key of class A.
11d. emitting a secure access signal conveying information dependent upon said accessibility attribute; and	The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.         For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys:

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 105 of 232

<u>Claim 11</u>	Accused Instrumentalities
	<ul> <li>"sepOS can then use the ephemeral wrapping key to wrap file keys for use by the Application</li> <li>Processor file-system driver. When the file-system driver reads or writes a file, it sends the wrapped key to the AES Engine."</li> <li>(Ex. A, Apple Platform Security, at 14.)</li> </ul>
	"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. [] When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." ( <i>Id.</i> at 85.)
	The signal with the ephemerally re-encrypted file keys is a secure signal because it comes from the Secure Enclave and thus from a secure environment. Furthermore, the signal is secure because the transmitted information is encrypted. The emitted file keys are encrypted with the ephemeral key:
	"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. At startup, the Secure Enclave negotiates an ephemeral key with the AES Engine. When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." ( <i>Id.</i> )

Claim 11	Accused Instrumentalities
	Filesystem Data Protection
	Overview
	File blocks are encrypted using AES-XTS with 128-bit keys
	Each file on the user partition is encrypted using a unique random key chosen by SE
	Raw file keys are never exposed to the AP
	<ul> <li>Wrapped with a key from the user keybag for long-term storage</li> </ul>
	<ul> <li>Wrapped with an ephemeral key while in use, bound to boot session (Ex. B, Behind the Scenes with iOS Security, at 29.)</li> </ul>

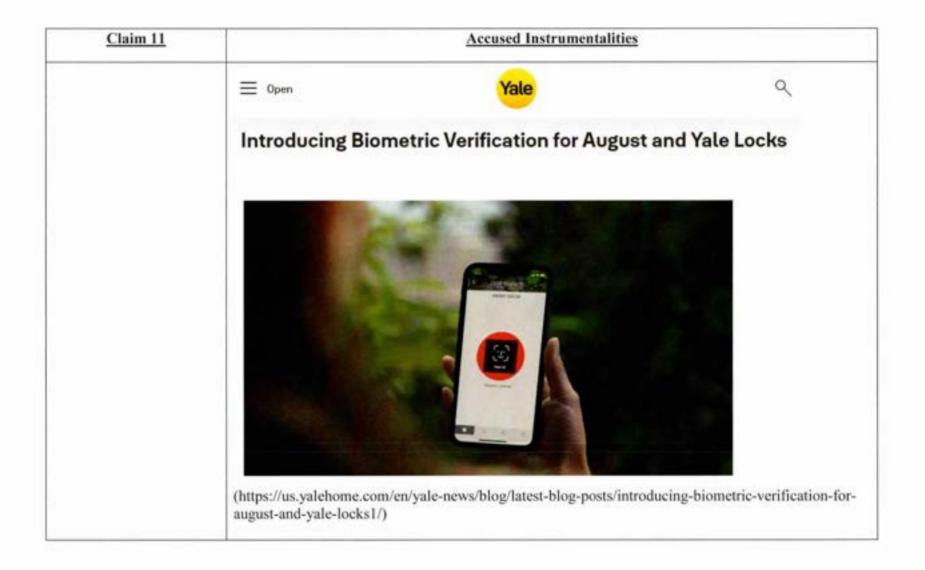


ASSA ABLOY Ex. 1021 - Page 106 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 108 of 232

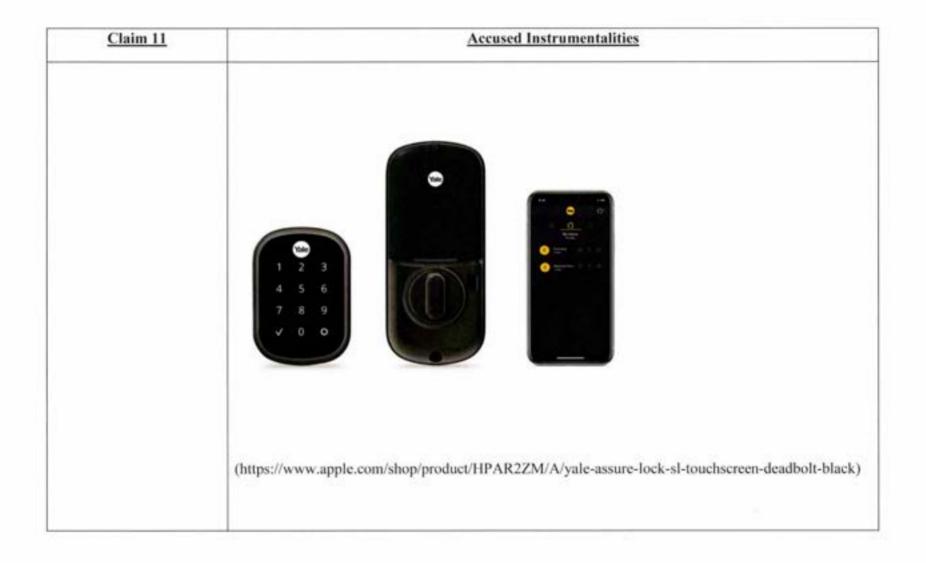
Claim 11	Accused Instrumentalities
11e. providing conditional access to the controlled item dependent upon said information, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.	The Accused Instrumentalities are configured to provide conditional access to the controlled item dependent upon said information, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device
	More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.
	"When the "Secure Remote Access" feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it."
	(https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for- august-and-yale-locks1/)

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 109 of 232



ASSA ABLOY Ex. 1021 - Page 108 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 110 of 232



Claim 12	Accused Instrumentalities
12. The method according to claim 11, wherein populating the database of biometric signatures further comprises enrolling a biometric signature into the database of biometric signatures, and wherein enrolling the biometric signature into the database comprises:	The Accused Instrumentalities are configured to enroll a biometric signature into the database of biometric signatures as set forth in elements 12a and 12b below.
12a. receiving a biometric signal; and	<ul> <li>The Accused Instrumentalities include a biometric sensor configured to receive the biometric signal.</li> <li>More specifically, the iPhone has at least one biometric sensor for capturing a fingerprint or a face (Touch ID and/or Face ID), namely a Touch ID sensor and a camera system with image sensor, respectively.</li> </ul>
	<ul> <li>Touch ID</li> <li>"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." <ul> <li>(Ex. A, Apple Platform Security, at 19.)</li> </ul> </li> <li>"Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the sensor continuing to expand the fingerprint map as additional overlapping nodes are identified with each use." <ul> <li>(Id.)</li> </ul> </li> <li>"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave."</li> </ul>

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 112 of 232

Claim 12	Accused Instrumentalities				
	( <i>Id.</i> )				
	The biometric sensor for Touch ID is located below the home button:				
	"The Home button is a stack of different materials, capped with a sapphire crystal lens. The surrounding stainless-steel ring works as a ground and detects the user's finger. This action activates a capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors." (https://appleinsider.com/inside/touch-id)				
	Laser-cut sapphire crysta Stainless steel detection ring Touch ID sensor				
	Tactile switch				
	Biometric sensor 121				
	"Where is the Touch ID sensor located?				
	The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.				
	(https://support.apple.com/en-us/HT201371)				

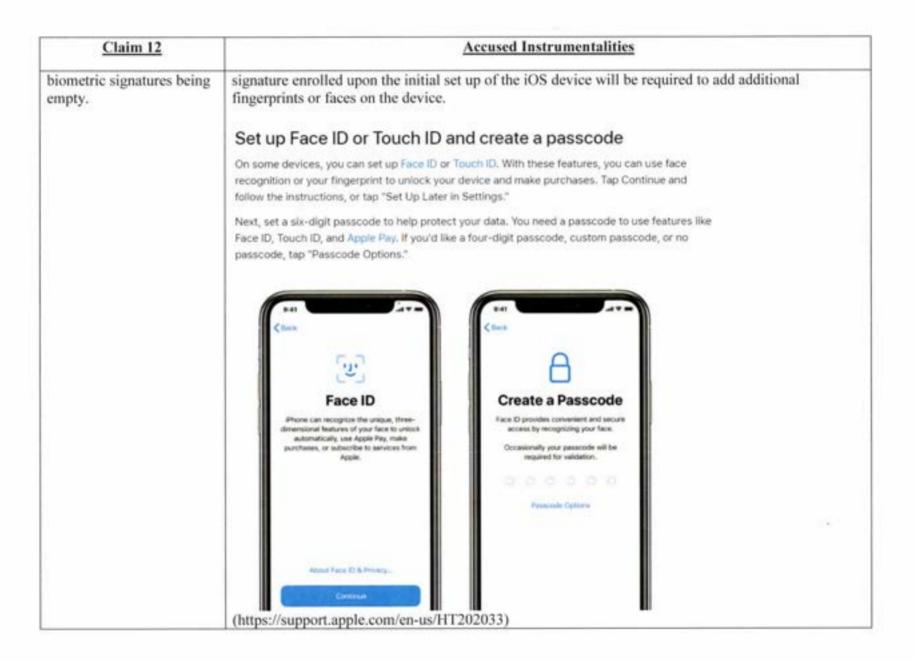
# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 113 of 232

<u>Claim 12</u>	Accused Instrumentalities
	The image sensor captures an 88-by-88-pixel, 500 PPI raster scan:
	"The 88-by-88-pixel, 500-ppi raster scan is temporarily stored in encrypted memory within the Secure Enclave while being vectorized for analysis, and then it's discarded. The analysis utilizes subdermal ridge flow angle mapping, which is a lossy process that discards minutia data that would be required to reconstruct the user's actual fingerprint. The resulting map of nodes is stored without any identity information in an encrypted format that can only be read by the Secure Enclave, and is never sent to Apple or backed up to iCloud or iTunes." (Ex. C, iOS Security white paper, at 8.)
	Face ID
	The biometric sensor for facial biometrics is a camera system ("TrueDepth camera system") with an image sensor.
	"With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face." (Ex. A, Apple Platform Security, at 20.)
	To receive a biometric signal, the camera system with image sensor reads over 30,000 infrared points to capture depth information along with a two-dimensional infrared image.
	"After the TrueDepth camera confirms the presence of an attentive face, it projects and <b>reads over</b> <b>30,000 infrared dots to form a depth map of the face along with a 2D infrared image</b> . This data is used to <b>create a sequence of 2D images and depth maps</b> , which are digitally signed and sent to the Secure Enclave. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 114 of 232

Claim 12	Accused Instrumentalities         mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." ( <i>Id.</i> , at 20.)         The camera system includes a biometric image sensor, namely a "CMOS image" sensor from Sony, to perform facial biometrics:				
	Structured light	Stilling to starting	C Ambient light		Characterine
	STM Pro CTL perturbation protection Tong Heating Via China Co	551: Nga	Mosure	Abelle Han-hal Cowell O-Min CADS more terror (MAD Son Langart Genks Association Koncerta INTK	Abohan LO Innotek Epitholia Epitholia Monarii MCDEL Jonaton Manarii Minaemi Diffectus Contral Evenents TSMC (patterning) Xintes (placking & cutting) Vivera (ITO) Vivera (ITO) Vivera (ITO)
	1.11.11.11.1		Active alignment		Vari Adva algoment equipment; ADM Pacific
	(https://appleinsider.co	om/articles/1	• ()	kings-of-apples-f	ace-id-camera-detailed-in-
	report)				1 - 11
2b. enrolling the iometric signal as an dministrator signature in esponse to the database of	The Accused instrumentalities are configured to enroll the biometric signal as an administrator signature in response to the database of biometric signatures being empty. More specifically, upon information and belief, the iPhone allows the users to enroll their biometric signature as an administrator when the user is setting up their first iOS device. The biometric				

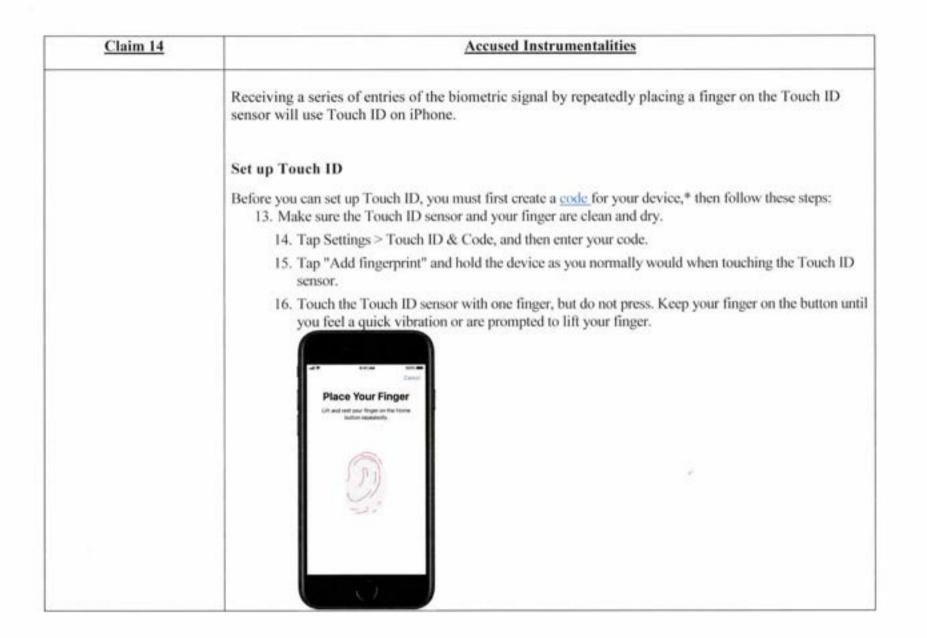
## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 115 of 232



.

<u>Claim 14</u>	Accused Instrumentalities		
14. A non-transitory computer readable storage medium storing a computer program comprising instructions, which when executed by processors causes the processors to:	The Accused Instrumentalities are non-transitory computer readable storage medium storing a computer program comprising instructions as set forth below.		
14a. receive a series of entries of a biometric signal;	The Accused Instrumentalities include a transmitter sub-system controller configured to receive a series of entries of the biometric signal.		
5151141,	More specifically, the Secure Enclave of the iPhone with the Secure Enclave Processor forms the means for receiving a series of entries of the biometric signal.		
	"Apple's biometric security architecture relies on a strict separation of responsibilities between the biometric sensor and the Secure Enclave, and a secure connection between the two. The sensor captures the biometric image and securely transmits it to the Secure Enclave." (Ex. A, Apple Platform Security, at 19.)		
	Touch ID		
	When a finger is placed on the biometric sensor, the finger is scanned and the corresponding biometric signal entry is received by the Secure Enclave.		
	"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave." ( <i>Id.</i> )		
	To enroll a fingerprint in the database, the iPhone's fingerprint sensor records an entry of a biometric signal when the user places his finger on the sensor. This is done multiple times, resulting in a series o entries of such biometric signals.		

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 117 of 232



Claim 14	Accused Instrumentalities		
	17. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.		
	18. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you would during the first scan."		
•	(https://support.apple.com/en-us/HT201371)		
	Accordingly, the user is prompted to place his finger on the sensor several times, in particular in accordance with step 5. Each time the finger is placed on the sensor, a corresponding biometric entry is generated, i.e. a series of such entries. All these entries, which result from placing the same finger on the sensor, form a series.		
	Face ID		
	The means for receiving a series of entries of the biometric signal includes a Secure Neural Engine, which is protected by the Secure Enclave. The Secure Neural Engine transforms the series of entries of the biometric signal received by the Secure Enclave into a biometric signature ("mathematical representation").		
	"After the TrueDepth camera confirms the presence of an attentive face, it projects and reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image. This data is used to create <b>a sequence of 2D images and depth maps</b> , which are digitally signed and <b>sent to the Secure Enclave</b> . To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the <b>Secure Neural Engine-protected</b> within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)		

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 119 of 232

Claim 14	Accused Instrumentalities		
	Each entry of the biometric signal thus contains a two-dimensional infrared image with 30,000 infrared points for capturing depth information. By continuously capturing such infrared images into a Face ID scan while the user moves his head into different poses, a series of entries of the biometric signal results. Two such Face ID scans are required to generate a biometric signature of a single face, so that two series of entries of the biometric signal are received accordingly.		
	Using Face ID on iPhone		
	1. Tap Settings > Face ID & Code. Enter your code when prompted.		
	2. Tap on "Configure Face ID".		
	3. Hold the device in portrait mode in front of your face and tap "Let's go".		
	4. Make sure your face is inside the frame and slowly move your head until the circle shown is completed. If you can't move your head, tap on "Options for operating aids".		
	5. After performing the first Face ID scan, tap "Next".		
	6. Again, slowly describe a circle with your head until it is completed.		
	7. Tap "Done."		
	(https://support.apple.com/en-us/HT208109)		
	The biometric signature of a single face is thus determined by two successive Face ID scans, each of which receives a series of entries of the biometric signal (compare steps 4. and 6. above).		
	To register a second face, the iPhone offers a corresponding option in its settings. If the user selects the option "Set up an alternative appearance" as shown in the figure below on https://www.macworld.co.uk/how-to/second-face-id-3803421/, a second face is registered by the iPhone in the same way as the first face.		

### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 120 of 232

Claim 14	Accused Instrumentalities			
	< Setting: Face ID & Passcode			
	(w)			
	UNL FACE ID FOR.			
	Phone Unlock			
	iTunges App Store			
	Apple			
	Passwo stoFil C			
	Other Ap. 4-Appm 1			
	Affairs of the first sectors. The sectors and advect sectors advect			
	Set Up an Alternative Appearance			
	en antiklikar for confirmanally inserving fram ynin hole. Form El cam recongrises wit afterwalten agesterfanott			
	Resart Face 12			
	Antischen Abention for Face ID			
	Hegune Admittan for Face to			
	The series of entries of the biometric signal is identified on the iPhone by both the number and duration of each such entry.			
	Touch ID			
	According to step 5 of the instructions https://support.apple.com/en-us/HT201371, for the enrollment of a single finger, the user has to repeatedly place the respective finger on the sensor and thus a number of entries in a row predetermined via the user guidance are captured by the iPhone. Each one of the entries must also be of a predetermined duration given to the user via the iPhone display, i.e. the user's finger must remain on the sensor for a predetermined duration for each entry of the biometric signal in order to capture the biometric signal during this time.			

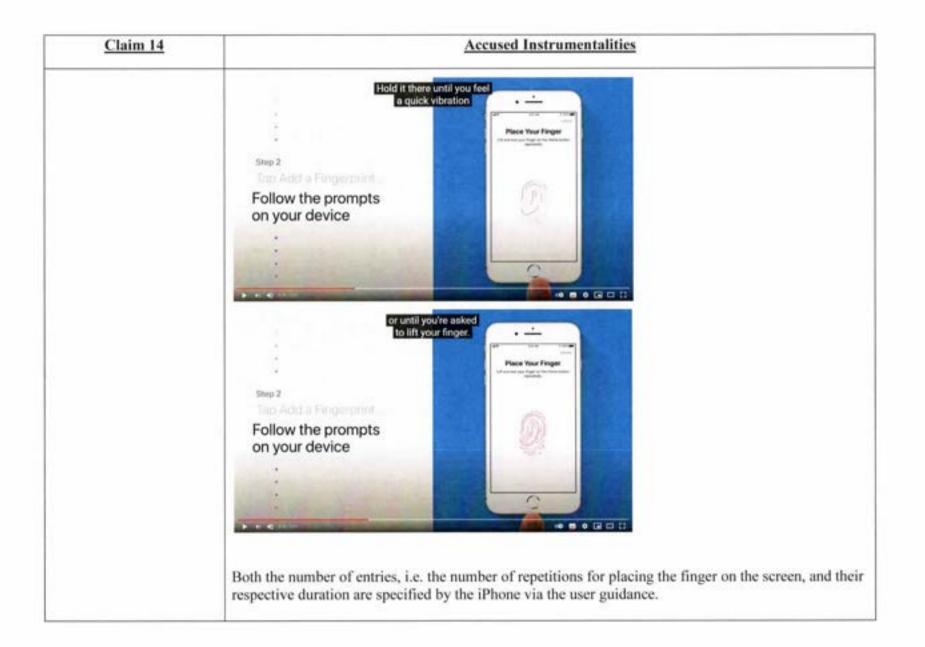
# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 121 of 232

Claim 14	Accused Instrumentalities				
	Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone and iPad.				
	Set up Touch ID				
	<ul> <li>4. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</li> </ul>				
	241 MA 100 mm Corker				
	Place Your Finger Lit and rest your farger on the Home button repeatedly.				
	5. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.				
	6. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you did during the first scan.				
	(https://support.apple.com/en-us/HT201371)				

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 122 of 232

<u>Claim 14</u>	Accused Instrumentalities	
<u></u>	After placing a finger on the home button, a fingerprint appears on the display with red progress bars spreading along some of the papillary bars until the capture of the biometric entry in question is complete:	
	ud ♥ ♦ 41 A44 X00x 000- Carker	
	Place Your Finger Lift and rest your finger on the Home button repeatedly.	
	When the required duration is reached, the iPhone vibrates after an entry of the biometric signal is received or it issues a prompt to the user to lift the finger. The user then lifts the finger in question and replaces the same finger so that the iPhone receives a series of biometric signal entries of sufficient duration for that finger. The process is repeated for the same finger for as long as required according to the iPhone's user guidance.	
	This is shown in the Apple You Tube video (32) How to set up Touch ID on your iPhone or iPad - Apple Support - YouTube (https://www.youtube.com/watch?v=xTZ2LALWZlg):	

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 123 of 232



ASSA ABLOY Ex. 1021 - Page 122 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 124 of 232

	Accused Instrumentalities			
	Face ID         The user moves his face in front of the camera to strike different poses, and the camera system with image sensor continuously captures a large number of biometric entries, i.e. here the 2D images with depth information, in a row.         "This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses."         (Ex. A, Apple Platform Security, at 20.)			
	The sufficient duration of an entry for a pose, i.e. an angular position of the head specified via the user interface of the iPhone, is indicated to the user by the transformation of a gray line into a green line:			
	Image: second			
4b. determine at least o f a number of said entri				

Claim 14	Accused Instrumentalities
and a duration of each of	
said entries;	More specifically, as discussed above, both Face ID and Touch ID require a specific number of entries to enroll a Touch ID or Face ID. The Accused Instrumentalities must determine that the specific number of entries have been input. Likewise, while not necessary for the claim, upon information and belief, the Accused Instrumentalities determine that each input of either facial or fingerprint data is of a sufficient duration. Again, when setting up Touch ID in the Accused Instrumentalities, the users are required to touch the home button with their finger several times for a certain duration. Similarly, the users need to scan their face twice, and each scan requires the users to move their head in a circle for a certain duration for Face ID.
	Touch ID: Register a fingerprint for Apple Touch ID by the user tapping a finger several times on the home button to record the fingerprint data.
	(https://video.search.yahoo.com/yhs/search?fr=yhs-pty-pty_converter&hsimp=yhs- pty_converter&hspart=pty&p=registering+
	fingerprint+apple+touch+id+on+screen+instructions#id=1&vid= 156de65ae06ca453643009fc0ea9cf79&action=click)
	Touch ID: The user's finger must remain on the home button long enough for the data to be recorded. "Touch the Touch ID sensor with your finger, but don't press it. Hold it there until you feel a quick vibration, or until you're asked to lift your finger." "Continue to lift and rest your finger slowly, making small adjustments to the position of your finger each time." (https://support.apple.com/en-au/HT201371)
	Touch ID: "you shouldn't tap too quickly or move your finger around" (https://support.apple.com/en-us/HT207537)
	Face ID: Setting up Face ID requires two scans of the user's face. Each scan asks users to move their head slowly in a circle to register different angles of the user's face. (https://www.imore.com/how-set-face-id-iphone)
14c. map said series into	The Accused Instrumentalities include a transmitter sub-system controller configured to map said
an instruction;	series into an instruction.

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 126 of 232

Claim 14	Accused Instrumentalities
	More specifically, the Secure Enclave of the iPhone contains means to assign the received row to an instruction: The Secure Enclave, after receiving the full set of entries of the biometric signal, assigns this set to an instruction for processing, encrypting and storing the biometric signature ("Touch ID and Face ID template data").
	"The sensor captures the biometric image and securely transmits it to the Secure Enclave. During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Ex. A, Apple Platform Security, at 19.)
	To carry out this instruction, the Secure Enclave has its own processor: "The Secure Enclave Processor provides the main computing power for the Secure Enclave." ( <i>Id.</i> , at 10.)
	Touch ID
	The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.
	"The analysis uses subdermal ridge flow angle mapping, a lossy process that discards "finger minutiae data" that would be required to reconstruct the user's actual fingerprint. During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches, but without any identity information." ( <i>Id.</i> , at 19.)
	<b>Face ID</b> The instruction involves the transformation of the set of entries of the biometric signal captured via the Face ID scans into a mathematical representation, i.e. the biometric signature of the face in question by the Secure Neural Engine of the Secure Enclave, as well as its encryption and storage.

<u>Claim 14</u>	Accused Instrumentalities
	"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses. " ( <i>Id.</i> , at 20.)
	"Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device. It's not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:
	<ul> <li>The mathematical representations of a user's face calculated during enrollment</li> <li>"</li> <li>(<i>Id.</i>, at 23.)</li> </ul>
14d. populate a database of biometric signatures according to the	The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.
instruction;	More specifically, the Secure Enclave stores the biometric signature, i.e. the encrypted mathematical representation of the fingerprint or face, in the database 105, i.e. the "secure nonvolatile storage":
	"The secure nonvolatile storage is used for all anti-replay services in the Secure Enclave. Anti-replay services on the Secure Enclave are used for revocation of data over events that mark anti-replay boundaries including, but not limited to, the following:
	<ul> <li></li> <li>Adding or removing a Touch ID fingerprint or Face ID face".</li> <li>(Ex. A, Apple Platform Security, at 16.)</li> </ul>
	"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." ( <i>Id.</i> , at 19.)

Claim 14	Accused Instrumentalities	
<u>Claim 14</u> 14e. receive the biometric signal;	Touch ID         "During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches"         (Id.)         Face ID         The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:         • The mathematical representations of a user's face calculated during enrollment".         (Id., at 23.)         The Accused Instrumentalities include a biometric sensor configured to receive the biometric signal.	
signal;	<ul> <li>More specifically, the iPhone has at least one biometric sensor for capturing a fingerprint or a face (Touch ID and/or Face ID), namely a Touch ID sensor and a camera system with image sensor, respectively.</li> <li><b>Touch ID</b></li> <li>"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.)</li> <li>"Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the <b>sensor</b> continuing to expand the fingerprint map as additional overlapping nodes are identified with each use." (<i>Id.</i>)</li> </ul>	
	"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave."	

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 129 of 232

Claim 14	Accused Instrumentalities	
	( <i>ld.</i> )	
	The biometric sensor for Touch ID is located below the home button:	
	"The Home button is a stack of different materials, capped with a sapphire crystal lens. The surrounding stainless-steel ring works as a ground and detects the user's finger. This action activates a capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors." (https://appleinsider.com/inside/touch-id)	
	Laser-cut sapphire crysta Stainless steel detection ring	
	Touch ID sensor Tactile switch	
	Biometric sensor 121	
	"Where is the Touch ID sensor located?	
	The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.	
	(https://support.apple.com/en-us/HT201371)	

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 130 of 232

<u>Claim 14</u>	Accused Instrumentalities
	The image sensor captures an 88-by-88-pixel, 500 PPI raster scan:
	"The 88-by-88-pixel, 500-ppi raster scan is temporarily stored in encrypted memory within the Secure Enclave while being vectorized for analysis, and then it's discarded. The analysis utilizes subdermal ridge flow angle mapping, which is a lossy process that discards minutia data that would be required to reconstruct the user's actual fingerprint. The resulting map of nodes is stored without any identity information in an encrypted format that can only be read by the Secure Enclave, and is never sent to Apple or backed up to iCloud or iTunes." (Ex. C, iOS Security white paper, at 8.)
	Face ID
	The biometric sensor for facial biometrics is a camera system ("TrueDepth camera system") with an image sensor.
	"With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face. " (Ex. A, Apple Platform Security, at 20.)
	To receive a biometric signal, the camera system with image sensor reads over 30,000 infrared points to capture depth information along with a two-dimensional infrared image.
	"After the TrueDepth camera confirms the presence of an attentive face, it projects and <b>reads over</b> <b>30,000 infrared dots to form a depth map of the face along with a 2D infrared image</b> . This data is used to <b>create a sequence of 2D images and depth maps</b> , which are digitally signed and sent to the Secure Enclave. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 131 of 232

Claim 14	Accused Instrumentalities	
	mathematical representation and compares that representation to t facial data is itself a mathematical representation of the user's face ( <i>Id.</i> , at 20.) The camera system includes a biometric image sensor, namely a " perform facial biometrics:	e captured across a variety of poses."
	Structured light	sera
	Montres Montres Montres Montres Montres Montres Montres Montres Coveril. Or CMUG image answer (1,410) VCIEL. STM Phage	Abrilder LG invaties
	CO (Instruction white) Care Large Active Large Active Large Active Large Active Large Active Large Active A	VCSEL romania Lumentum
	Cherton Contante Cont	VCSEL brock-chord: Winseeni Driftactive Ostical Element; TSMO (patterning) Xintee (stacking & surting) Vinera (ITO) Water level context III surfaces) Haptagon/ AMS
	Active alignment	Enter: Viewi Active adarment equipment
		ASM Pacific
	(https://appleinsider.com/articles/17/09/09/inner-workings-of-app report)	les-face-id-camera-detailed-in-
4f. match the biometric gnal against members of the database of biometric gnatures to thereby	The Accused Instrumentalities include a transmitter controller of signal conveying information dependent upon said accessibility	

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 132 of 232

Claim 14	Accused Instrumentalities
output an accessibility attribute;	More specifically, the iPhone's System on Chip (SOC), i.e. the Secure Enclave with its Secure Enclave Processor (SEP) or a Secure Neural Engine contained therein, is a means (103) to check a match of the biometric signal with elements of the biometric signature database.
	"The Secure Enclave is a system on chip (SoC) that is included on all recent iPhone, devices" (Ex. A, Apple Platform Security, at 7.)
	"During <b>matching</b> , the Secure Enclave <b>compares</b> incoming data from the biometric sensor against the stored templates <b>to determine whether to unlock the device</b> or respond that a match is valid (for Apple Pay, in-app, and other uses of Touch ID and Face ID). " ( <i>Id.</i> , at 19.)
	The biometric signal received from the biometric sensor ("incoming data from the biometric sensor") is thus checked by the Secure Enclave and its SEP with the elements of the database of biometric signatures 105, i.e. the "stored templates", for the presence of a match.
	For Touch ID, the Secure Enclave match verification is performed as follows:
	"The Secure Enclave is responsible for processing fingerprint data from the Touch ID sensor, determining if there is a match against registered fingerprints, and then enabling access or purchases on behalf of the user" (Ex. C, iOS Security white paper, at 7.)
	"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches" (Ex. A, Apple Platform Security, at 19.)
	"Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. " (https://support.apple.com/en-us/HT204587)

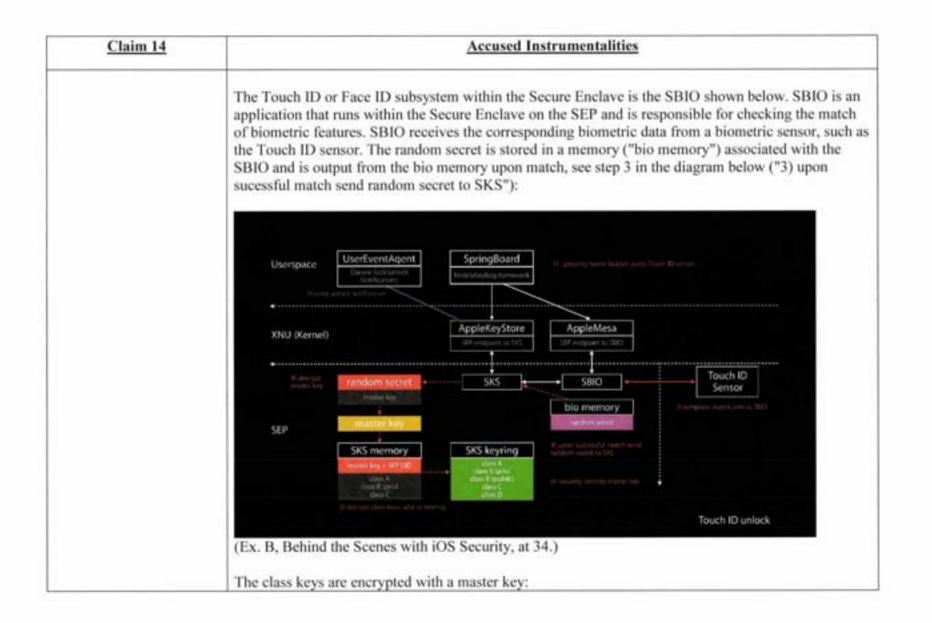
# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 133 of 232

<u>Claim 14</u>	Accused Instrumentalities
	"Touch ID can read multiple fingerprints and recognize fingerprints at any orientation of the finger. The system then creates a mathematical representation of your fingerprint and compares it to the registered fingerprint data to determine a match and unlock your device." (https://support.apple.com/de-de/HT204587)
	For <b>Face ID</b> , the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:
	"Face ID uses neural networks for determining attention, <b>matching</b> , and antispoofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)
	"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." ( <i>Id.</i> ).
	"Facial matching security
	Facial matching is performed within the Secure Enclave using neural networks trained specifically for that purpose Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device." ( <i>Id.</i> at 23.)
	When the Secure Enclave, or more precisely the Touch ID or Face ID subsystem within the Secure Enclave, has determined that a match exists, an accessibility attribute is issued by the corresponding Touch ID or Face ID subsystem. This Touch ID or Face ID subsystem is also referred to as the SBIO. The accessibility attribute confirms that there is a match and that the iPhone is to be unlocked (" determine whether to unlock the device").

Claim 14	Accused Instrumentalities
	This confirmation of the match is signaled by the SBIO by issuing a random secret to which only the Touch ID or Face ID subsystem within the Secure Enclave has access:
	"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device []." ( <i>Id.</i> at 19.)
	"Uses for Touch ID and Face ID
	Unlocking a device or user account
	[] keys for the highest class of Data Protection-which are held in the Secure Enclave [].
	With Touch ID or Face ID enabled, the keys aren't discarded when the device or account locks; instead, they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the Secure Enclave. When a user attempts to unlock the device or account, if the device detects a successful match, it provides the key for unwrapping the Data Protection keys, and the device or account is unlocked. This process provides additional protection by requiring cooperation between the Data Protection and Touch ID or Face ID subsystems to unlock the device."
	( <i>Id.</i> at 24.)
	"The class key is protected with the hardware UID and, for some classes, the user's passcode." ( <i>Id.</i> at 85.)
	"Complete Protection
	(NSFileProtectionComplete): The class key is protected with a key derived from the user passcode or password and the device UID. Shortly after the user locks a device (10 seconds, if the Require Password setting is Immediately), the decrypted class key is discarded, rendering all data in this class inaccessible until the user enters the passcode again or unlocks (logs in to) the device using Touch ID or Face ID."
	( <i>Id.</i> at 86.)

ASSA ABLOY Ex. 1021 - Page 133 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 135 of 232



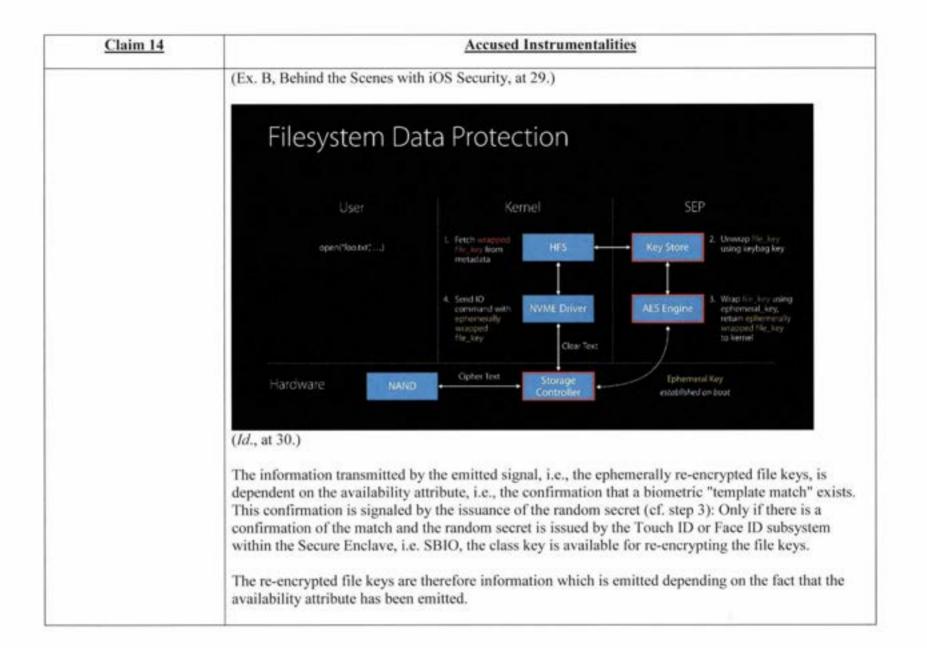
ASSA ABLOY Ex. 1021 - Page 134 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

Claim 14	Accused Instrumentalities	
	User Keybags	
	Background	
	Sets of keys generated for each user to protect their data at rest	
	Keys wrapped by master key derived from user passcode and SEP UID	
	After 10 incorrect passcode entries, SEP will not process any further attempts	
	Different policy associated with each keybag key—Usage, availability	
	( <i>Id.</i> , at 25.)	
	The random secret is issued to SKS. SKS is a Secure Key Service application which is located within the Secure Enclave on the SEP and is responsible for decrypting class keys. The random secret provided by SBIO is used to decrypt a master key ("4) decrypt master key"). The master key is concatenated with the UID of the SEP and thus class keys are decrypted and added to the SKS keyring ("5) decrypt class keys, add to keyring") for further use by the Secure Enclave. The decrypted class keys include, for example, the class key of class A.	
14g. emit a secure access signal conveying information dependent upon said accessibility	The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.         For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys:	
attribute; and	"sepOS can then use the ephemeral wrapping key to wrap file keys for use by the Application Processor file-system driver. When the file-system driver reads or writes a file, it sends the wrapped key to the AES Engine."	

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 137 of 232

Claim 14	Accused Instrumentalities
	(Ex. A, Apple Platform Security, at 14.)
	"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. [] When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." ( <i>Id.</i> at 85.)
	The signal with the ephemerally re-encrypted file keys is a secure signal because it comes from the Secure Enclave and thus from a secure environment. Furthermore, the signal is secure because the transmitted information is encrypted. The emitted file keys are encrypted with the ephemeral key:
	"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. At startup, the Secure Enclave negotiates an ephemeral key with the AES Engine. When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key an sent back to the Application Processor." ( <i>Id.</i> )
	Filesystem Data Protection
	Overview
	File blocks are encrypted using AES-XTS with 128-bit keys
	Each file on the user partition is encrypted using a unique random key chosen by SE
	Raw file keys are never exposed to the AP
	<ul> <li>Wrapped with a key from the user keybag for long-term storage</li> </ul>
	<ul> <li>Wrapped with an ephemeral key while in use, bound to boot session</li> </ul>

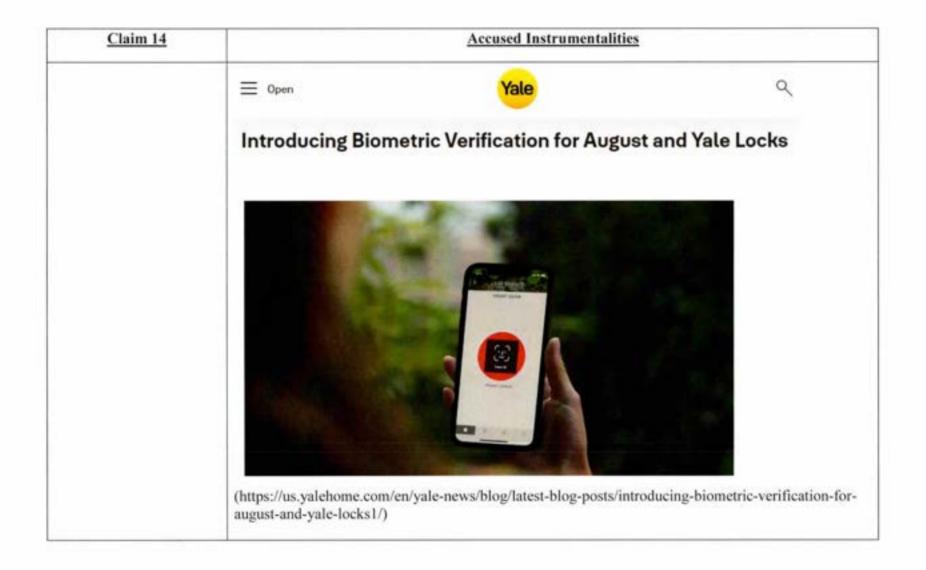
#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 138 of 232



## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 139 of 232

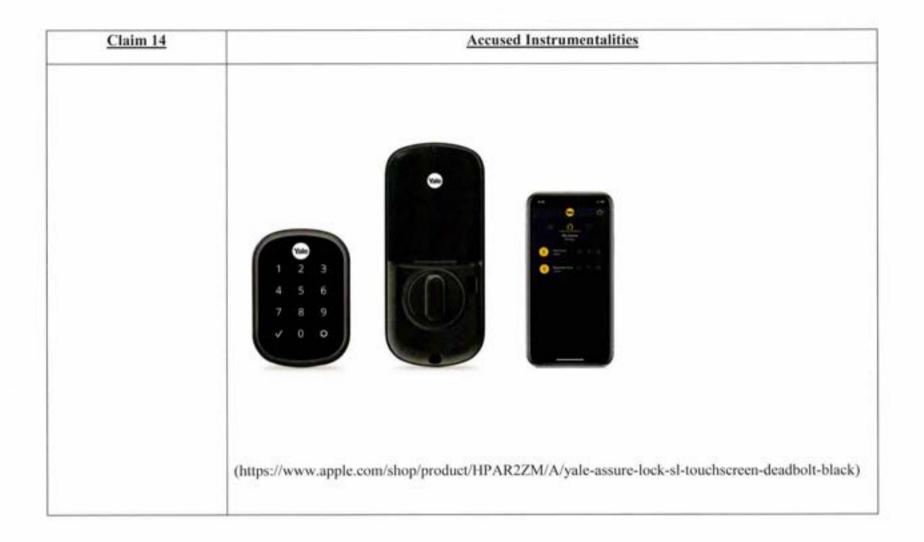
Claim 14 Accused Instrumentalities	
14h. provide conditional access to a controlled item dependent upon said information, wherein the	The Accused Instrumentalities are configured to provide conditional access to a controlled item dependent upon said information, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.
controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing	More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.
device.	"When the "Secure Remote Access" feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it."
	(https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for- august-and-yale-locks1/)

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 140 of 232



ASSA ABLOY Ex. 1021 - Page 139 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 141 of 232



# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 142 of 232

Claim 15	Accused Instrumentalities
<ol> <li>A system for providing secure access to a controlled item, the system comprising:</li> </ol>	The Accused Instrumentalities are non-transitory computer readable storage medium storing a computer program comprising instructions as set forth below.
5a. a memory comprising a database of biometric signatures;	The Accused Instrumentalities include a memory comprising a database of biometric signatures.         More specifically, the iPhone allows multiple biometric signatures to be entered into a database on the iPhone:         Touch ID         The iPhone allows the registration of multiple fingerprints:         Image:

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 143 of 232

Claim 15	Accused Instrumentalities
	"Register up to five fingerprints."
	"Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. " (https://support.apple.com/en-us/HT204587)
	"Touch ID can read multiple fingerprints and recognize fingerprints at any orientation of the finger. The system then creates a mathematical representation of your fingerprint and compares it to the registered fingerprint data to determine a match and unlock your device." (https://support.apple.com/en-us/HT204587)
	Face ID
	The iPhone allows the registration of multiple faces:

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 144 of 232

Claim 15	Accused Instrumentalities
	The main and su schließen
	To register a face, the iPhone takes a series of pictures of the user in different poses while circling his head. This is revealed in detail in https://support.apple.com/en-us/HT208109 in the second section "Configure Face ID", there also the figure shown above.
	To register a second face, the iPhone offers a corresponding option in its settings. If the user selects the option "Set up an alternative appearance" as shown in the figure below (from How To Add A Second Face To Face ID - Macworld UK; https://www.macworld.co.uk/how-to/second-face-id-3803421/), a second face is registered by the iPhone in the same way as the first face.
	"Set up Face ID or add another face.
	<ul> <li>Select "Settings" &gt; "Face ID &amp; Code" &gt; "Configure alternate appearance" if you want to configure another face to be recognized by Face ID."</li> </ul>

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 145 of 232

Claim 15	Accused Instrumentalities
	(https://support.apple.com/de-de/guide/iphone/iph6d162927a/ios)
	Carting Face ID & Pesscode
	(E)
	iPhone Unlock
	Apple
	Passwork utofill Converted A Appoint
	Present care in a constraint of the attingent from the maximum of the second se
	Set Up an Atternative Approximation In addition to continuously learning free any test, finite IS internetization approximation approximation approximation
	Result Face (D)
	Attinuities Require Attention for Face ID
	The page How To Add A Second Face To Face ID - Macworld UK (https://www.macworld.co.uk/how-to/second-face-id-3803421/) literally states:
	"Face ID is a fast and secure way to unlock your iPhone or iPad Pro, but you may not know that you can actually set up more than one face to use the feature.

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 146 of 232

Claim 15	Accused Instrumentalities
	This second face could belong to a loved one, enabling your partner or child to access your phone without requiring your smiling mug to unlock it. "
	To store the biometric signatures ("template data") from the received biometric signals, the iPhone has a System on Chip (SOC) called a Secure Enclave. A Secure Enclave Processor provides the Secure Enclave with computing power:
	"The Secure Enclave is a system on chip (SoC) that is included on all recent iPhone, devices" (Ex. A, Apple Platform Security, at 7.)
	"The Secure Enclave is a dedicated secure subsystem integrated into Apple systems on chip (SoCs)." ( <i>Id.</i> , at 9.)
	The Secure Enclave Processor provides the main computing power for the Secure Enclave." ( <i>Id.</i> , at 10.)
	"During enrollment, the Secure Enclave processes, encrypts, and <b>stores</b> the corresponding Touch ID and Face ID template data." ( <i>Id.</i> , at 19.)
	The Secure Enclave has access to a memory assigned to it and accessible only to it:
	Secure nonvolatile storage "The Secure Enclave is equipped with a dedicated secure nonvolatile storage device. The secure nonvolatile storage is connected to the Secure Enclave using a dedicated I2C bus, so that it can only be accessed by the Secure Enclave." ( <i>Id.</i> , at 15.)
	This memory serves as a database for storing the biometric signatures:

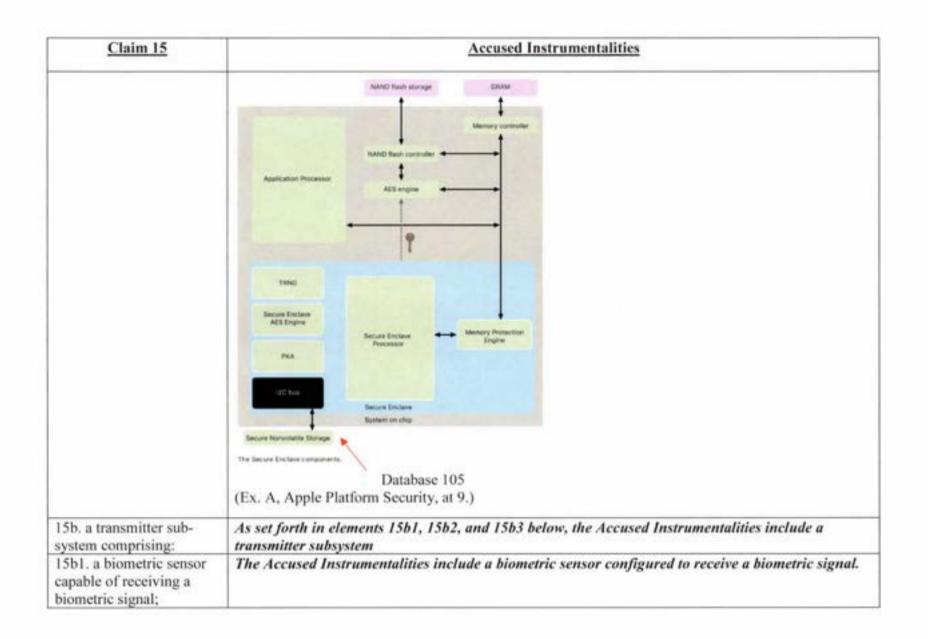
ASSA ABLOY Ex. 1021 - Page 145 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 147 of 232

Claim 15	Accused Instrumentalities
	"The secure nonvolatile storage is used for all anti-replay services in the Secure Enclave. Anti-replay services on the Secure Enclave are used for revocation of data over events that mark anti-replay boundaries including, but not limited to, the following:
	<ul> <li></li> <li>Adding or removing a Touch ID fingerprint or Face ID face".</li> </ul>
	( <i>Id.</i> , at 16.)
	This database is shown in the figure from Apple Platform Secutiry reproduced below:

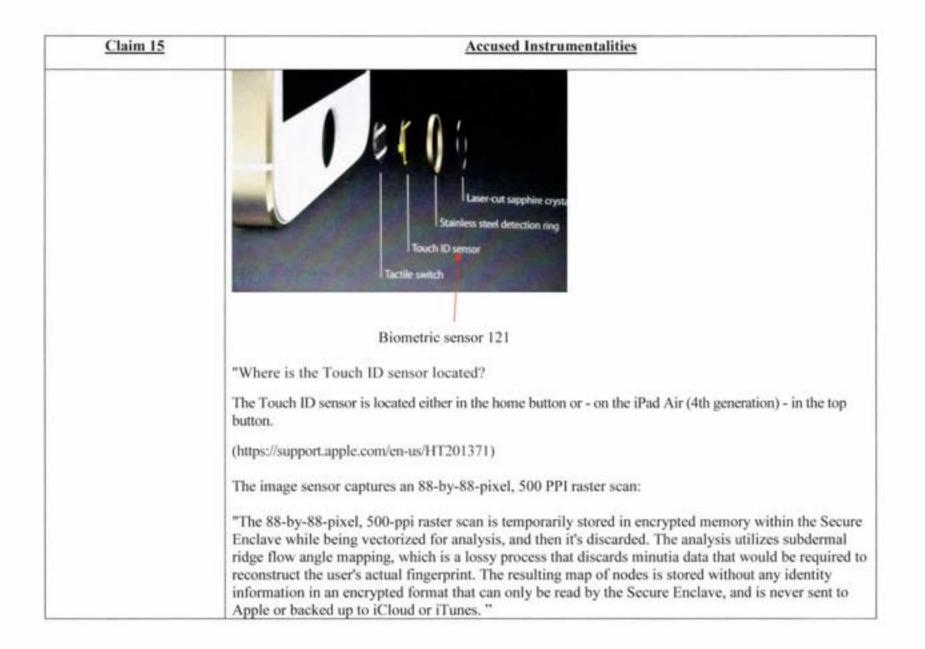
4,

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 148 of 232



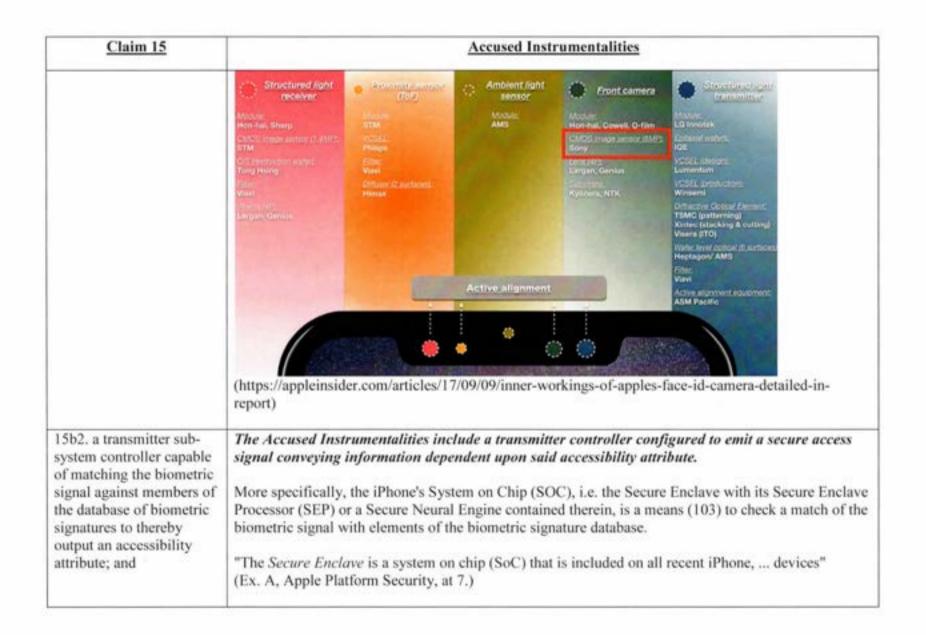
Claim 15	Accused Instrumentalities
	More specifically, the iPhone has at least one biometric sensor for capturing a fingerprint or a face (Touch ID and/or Face ID), namely a Touch ID sensor and a camera system with image sensor, respectively.
	Touch ID
	"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.)
	"Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the <b>sensor</b> continuing to expand the fingerprint map as additional overlapping nodes are identified with each use." ( <i>Id.</i> )
	"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave." ( <i>Id.</i> )
	The biometric sensor for Touch ID is located below the home button:
	"The Home button is a stack of different materials, capped with a sapphire crystal lens. The surrounding stainless-steel ring works as a ground and detects the user's finger. This action activates a capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors." (https://appleinsider.com/inside/touch-id)

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 150 of 232



Claim 15	Accused Instrumentalities
	(Ex. C, iOS Security white paper, at 8.)
	Face ID
	The biometric sensor for facial biometrics is a camera system (" <b>TrueDepth</b> camera <b>system</b> ") with an image sensor.
	"With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face. " (Ex. A, Apple Platform Security, at 20.)
	To receive a biometric signal, the camera system with image sensor reads over 30,000 infrared points to capture depth information along with a two-dimensional infrared image.
	"After the TrueDepth camera confirms the presence of an attentive face, it projects and <b>reads over</b> <b>30,000 infrared dots to form a depth map of the face along with a 2D infrared image</b> . This data is used to <b>create a sequence of 2D images and depth maps</b> , which are digitally signed and sent to the Secure Enclave. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." ( <i>Id.</i> )
	The camera system includes a biometric image sensor, namely a "CMOS image" sensor from Sony, to perform facial biometrics:

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 152 of 232



## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 153 of 232

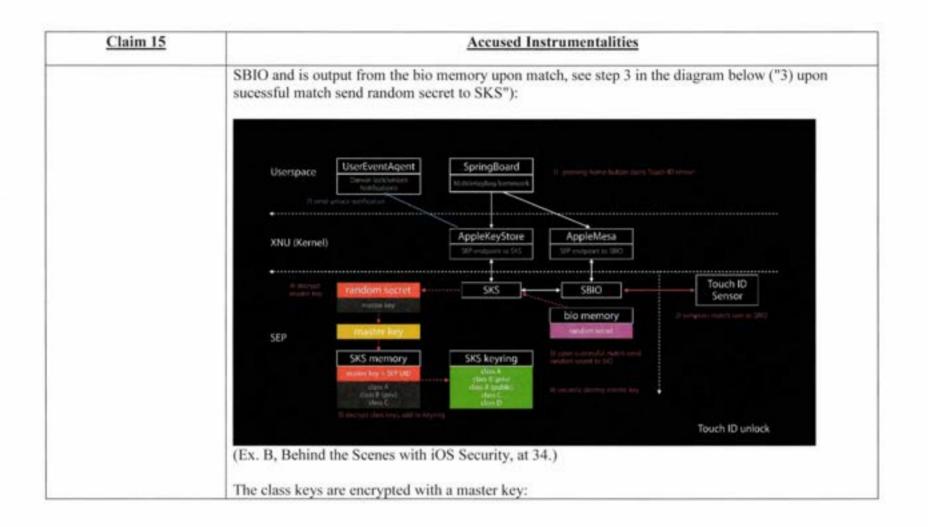
<u>Claim 15</u>	Accused Instrumentalities			
	"During <b>matching</b> , the Secure Enclave <b>compares</b> incoming data from the biometric sensor against the stored templates <b>to determine whether to unlock the device</b> or respond that a match is valid (for Apple Pay, in-app, and other uses of Touch ID and Face ID). " ( <i>Id.</i> , at 19.)			
	The biometric signal received from the biometric sensor ("incoming data from the biometric sensor") is thus checked by the Secure Enclave and its SEP with the elements of the database of biometric signatures 105, i.e. the "stored templates", for the presence of a match.			
	For Touch ID, the Secure Enclave match verification is performed as follows:			
	"The Secure Enclave is responsible for processing fingerprint data from the Touch ID sensor, determining if there is a match against registered fingerprints, and then enabling access or purchases on behalf of the user" (Ex. C, iOS Security white paper, at 7.)			
	"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches" (Ex. A, Apple Platform Security, at 19.)			
	"Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. " (https://support.apple.com/en-us/HT204587)			
	"Touch ID can read multiple fingerprints and recognize fingerprints at any orientation of the finger. The system then creates a mathematical representation of your fingerprint and compares it to the registered fingerprint data to determine a match and unlock your device." (https://support.apple.com/de-de/HT204587)			

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 154 of 232

Claim 15	Accused Instrumentalities			
	For <b>Face ID</b> , the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:			
	"Face ID uses neural networks for determining attention, <b>matching</b> , and antispoofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)			
	"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." ( <i>Id.</i> ).			
	"Facial matching security			
	Facial matching is performed within the Secure Enclave using neural networks trained specifically for that purpose Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device." ( <i>Id.</i> at 23.)			
	When the Secure Enclave, or more precisely the Touch ID or Face ID subsystem within the Secure Enclave, has determined that a match exists, an accessibility attribute is issued by the corresponding Touch ID or Face ID subsystem. This Touch ID or Face ID subsystem is also referred to as the SBIO. The accessibility attribute confirms that there is a match and that the iPhone is to be unlocked (" determine whether to unlock the device").			
	This confirmation of the match is signaled by the SBIO by issuing a random secret to which only the Touch ID or Face ID subsystem within the Secure Enclave has access:			
	"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device []." ( <i>Id.</i> at 19.)			

<u>Claim 15</u>	Accused Instrumentalities		
	"Uses for Touch ID and Face ID		
	Unlocking a device or user account		
	[] keys for the highest class of Data Protection-which are held in the Secure Enclave [].		
	With Touch ID or Face ID enabled, the keys aren't discarded when the device or account locks; instead, they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the Secure Enclave. When a user attempts to unlock the device or account, if the device detects a successful match, it provides the key for unwrapping the Data Protection keys, and the device or account is unlocked. This process provides additional protection by requiring cooperation between the Data Protection and Touch ID or Face ID subsystems to unlock the device."		
	( <i>Id.</i> at 24.)		
	"The class key is protected with the hardware UID and, for some classes, the user's passcode." ( <i>Id.</i> at 85.)		
	"Complete Protection		
	(NSFileProtectionComplete): The class key is protected with a key derived from the user passcode or password and the device UID. Shortly after the user locks a device (10 seconds, if the Require Password setting is Immediately), the decrypted class key is discarded, <b>rendering all data in this</b> <b>class inaccessible until the user</b> enters the passcode again or <b>unlocks</b> (logs in to) <b>the device using</b> <b>Touch ID or Face ID.</b> "		
	( <i>Id.</i> at 86.)		
	The Touch ID or Face ID subsystem within the Secure Enclave is the SBIO shown below. SBIO is an application that runs within the Secure Enclave on the SEP and is responsible for checking the match of biometric features. SBIO receives the corresponding biometric data from a biometric sensor, such as the Touch ID sensor. The random secret is stored in a memory ("bio memory") associated with the		

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 156 of 232



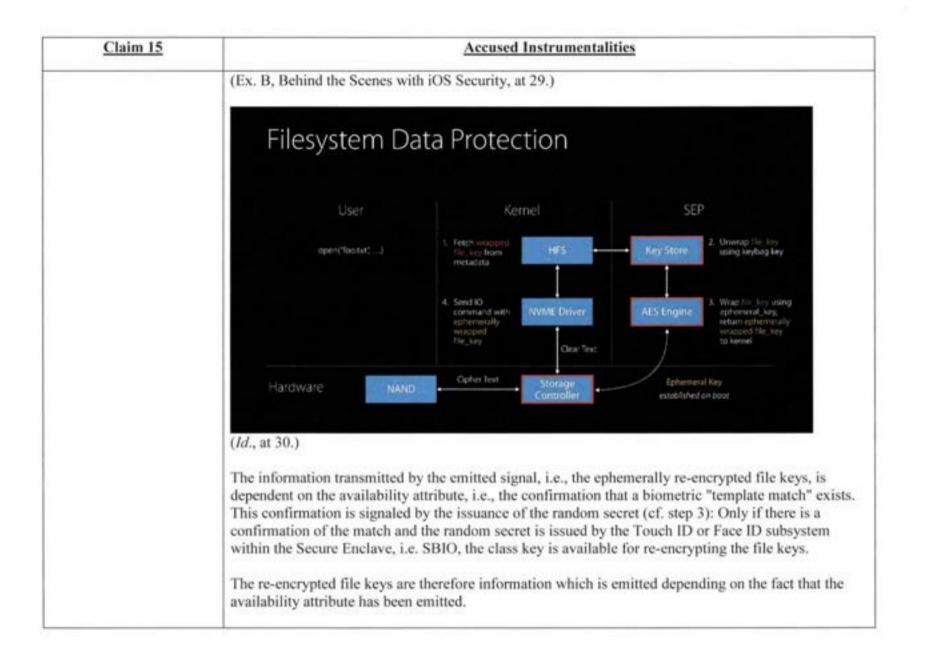
ASSA ABLOY Ex. 1021 - Page 155 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

Claim 15	Accused Instrumentalities		
	User Keybags		
	Background		
	Sets of keys generated for each user to protect their data at rest		
	Keys wrapped by master key derived from user passcode and SEP UID		
	After 10 incorrect passcode entries, SEP will not process any further attempts		
	Different policy associated with each keybag key—Usage, availability		
	( <i>Id.</i> , at 25.)		
	The random secret is issued to SKS. SKS is a Secure Key Service application which is located within the Secure Enclave on the SEP and is responsible for decrypting class keys. The random secret provided by SBIO is used to decrypt a master key ("4) decrypt master key"). The master key is concatenated with the UID of the SEP and thus class keys are decrypted and added to the SKS keyring ("5) decrypt class keys, add to keyring") for further use by the Secure Enclave. The decrypted class keys include, for example, the class key of class A.		
15b3. a transmitter capable of emitting a secure access signal	The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.		
conveying information	For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys:		
dependent upon said accessibility attribute; and	"sepOS can then use the ephemeral wrapping key to wrap file keys for use by the Application Processor file-system driver. When the file-system driver reads or writes a file, it sends the wrapped key to the AES Engine."		

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 158 of 232

Claim 15	Accused Instrumentalities				
	(Ex. A, Apple Platform Security, at 14.)				
	"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. [] When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." ( <i>Id.</i> at 85.)				
	The signal with the ephemerally re-encrypted file keys is a secure signal because it comes from the Secure Enclave and thus from a secure environment. Furthermore, the signal is secure because the transmitted information is encrypted. The emitted file keys are encrypted with the ephemeral key:				
	"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. At startup, the Secure Enclave negotiates an ephemeral key with the AES Engine. When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key an sent back to the Application Processor." ( <i>Id.</i> )				
	Filesystem Data Protection				
	Overview				
	File blocks are encrypted using AES-XTS with 128-bit keys				
	Each file on the user partition is encrypted using a unique random key chosen by SE				
	Raw file keys are never exposed to the AP				
	<ul> <li>Wrapped with a key from the user keybag for long-term storage</li> </ul>				
	<ul> <li>Wrapped with an ephemeral key while in use, bound to boot session</li> </ul>				

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 159 of 232



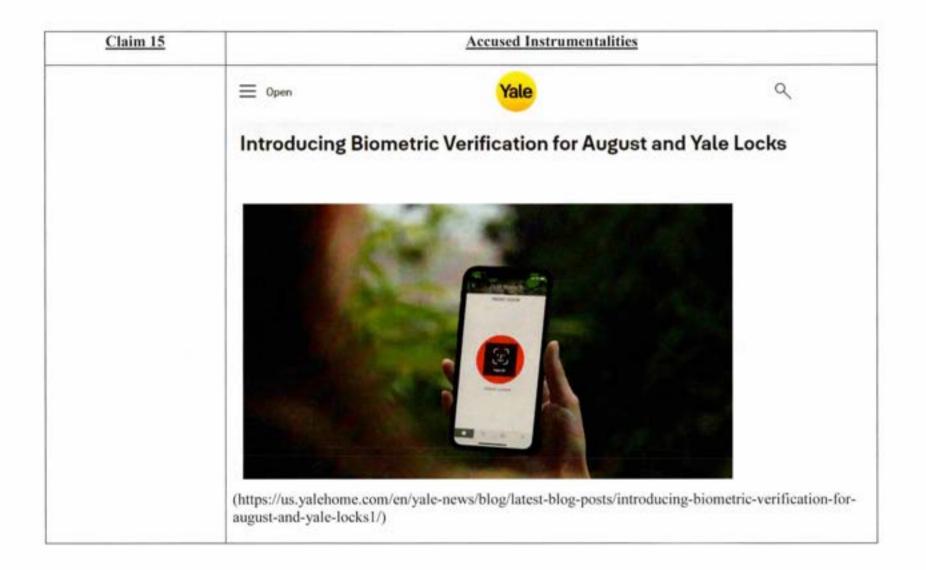
# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 160 of 232

Claim 15	Accused Instrumentalities				
15c. a receiver sub-system comprising:	As set forth in elements 15c1 and 15c2 below, the Accused Instrumentalities include a receiver sub- system.				
15c1. a receiver sub- system controller capable of: receiving the transmitted secure access signal; and	The Accused Instrumentalitie transmitted secure access signed An application processor (118 file key. To read files from the signal by creating a read come ephemerally wrapped file_key with AES engine). This read of to read and decrypt the encrypt Filesystem Data	nal. 8) with file system dr e NAND Flash stora; mand with the ephen y") and sends it to the command provides the poted file from the NA	iver, which r ge, the applic terally wrapp e storage con the storage co ND flash sto	eceives the ep ation process bed file key (" troller (109) ( ntroller with a	hemerally re-encrypted or processes the received IO command with NAND Flash controller
	User	Kernel		SEP	
	apen("foa.txt",)	L. Fetch wheepend his key from metacata	HFS +	Key Store	<ol> <li>Unwrap file, key using keybag key</li> </ol>
		4. Send IO command with ephernetally whapped file_key	Clear Text	AES Engine	3. What fire Jury unling ophermetal_key, return-splicemenally stapped file_key to iternel
	Hardware		Storage ontroller	Ephemera esablished	
	(Ex. B, Behind the Scenes with	th iOC Converter at 20	2.)		

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 161 of 232

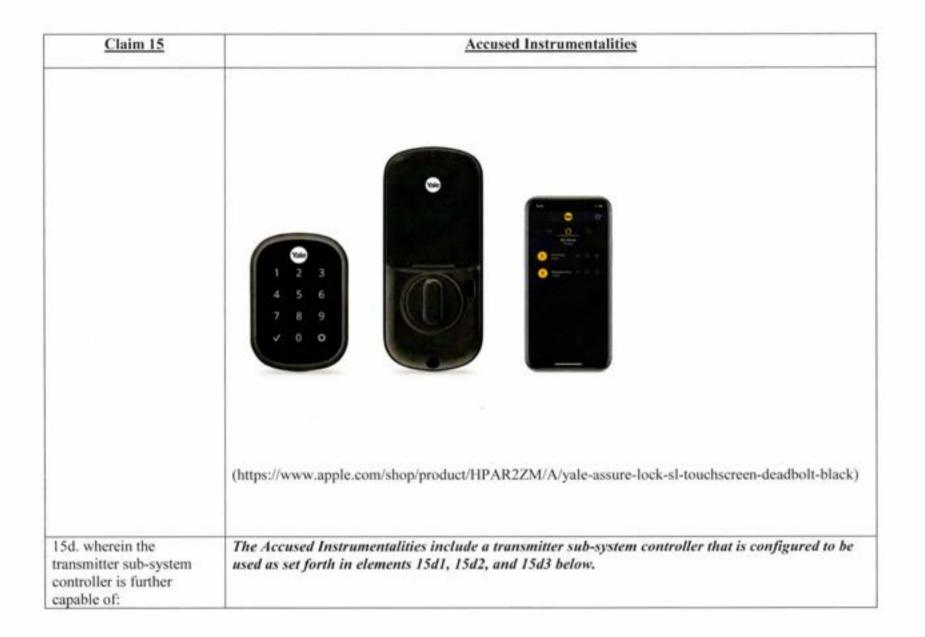
Claim 15	Accused Instrumentalities				
	"sepOS can then use the ephemeral wrapping key to wrap file keys for use by the Application Processor file-system driver. When the file-system driver reads or writes a file, it sends the wrapped key to the AES Engine." (Ex. A, Apple Platform Security, at 14.) "All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. [] When the Secure Enclave unwraps a file's keys, they're rewrapped with				
	the ephemeral key and sent back to the Application Processor." ( <i>Id.</i> , at 85.)				
15c2. providing conditional access to the controlled item dependent upon said information;	The Accused Instrumentalities include a receiver sub-system configured to provide conditional access to the controlled item dependent upon said information.				
	More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.				
	"When the "Secure Remote Access" feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it."				
	(https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for- august-and-yale-locks1/)				

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 162 of 232



ASSA ABLOY Ex. 1021 - Page 161 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 163 of 232



## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 164 of 232

Claim 15	Accused Instrumentalities
15d1. receiving a series of entries of the biometric signal, said series being characterised according to	The Accused Instrumentalities include a transmitter sub-system controller configured to receive a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry.
at least one of the number of said entries and a duration of each said	More specifically, the Secure Enclave of the iPhone with the Secure Enclave Processor forms the means for receiving a series of entries of the biometric signal.
duration of each said entry;	"Apple's biometric security architecture relies on a strict separation of responsibilities between the biometric sensor and the Secure Enclave, and a secure connection between the two. The sensor captures the biometric image and securely transmits it to the Secure Enclave." (Ex. A, Apple Platform Security, at 19.)
	Touch ID
	When a finger is placed on the biometric sensor, the finger is scanned and the corresponding biometric signal entry is received by the Secure Enclave.
	"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave." ( <i>Id.</i> )
	To enroll a fingerprint in the database, the iPhone's fingerprint sensor records an entry of a biometric signal when the user places his finger on the sensor. This is done multiple times, resulting in a series of entries of such biometric signals.
	Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone.
	Set up Touch ID
	Before you can set up Touch ID, you must first create a code for your device,* then follow these steps:

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 165 of 232

Claim 15	Accused Instrumentalities
	19. Make sure the Touch ID sensor and your finger are clean and dry.
	20. Tap Settings > Touch ID & Code, and then enter your code.
	21. Tap "Add fingerprint" and hold the device as you normally would when touching the Touch ID sensor.
	22. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.
	All V Bet MI WOY BE Care Place Your Finger Lift and rest your finger on the Home button repeatedly.
	23. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.
	24. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you would during the first scan."
	(https://support.apple.com/en-us/HT201371)

Claim 15	Accused Instrumentalities
	Accordingly, the user is prompted to place his finger on the sensor several times, in particular in accordance with step 5. Each time the finger is placed on the sensor, a corresponding biometric entry is generated, i.e. a series of such entries. All these entries, which result from placing the same finger on the sensor, form a series.
	Face ID
	The means for receiving a series of entries of the biometric signal includes a Secure Neural Engine, which is protected by the Secure Enclave. The Secure Neural Engine transforms the series of entries of the biometric signal received by the Secure Enclave into a biometric signature ("mathematical representation").
	"After the TrueDepth camera confirms the presence of an attentive face, it projects and reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image. This data is used to create <b>a sequence of 2D images and depth maps</b> , which are digitally signed and <b>sent to the Secure Enclave</b> . To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the <b>Secure Neural Engine-protected</b> within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)
	Each entry of the biometric signal thus contains a two-dimensional infrared image with 30,000 infrared points for capturing depth information. By continuously capturing such infrared images into a Face ID scan while the user moves his head into different poses, a series of entries of the biometric signal results. Two such Face ID scans are required to generate a biometric signature of a single face, so that two series of entries of the biometric signal are received accordingly.
	Using Face ID on iPhone
	1. Tap Settings > Face ID & Code. Enter your code when prompted.
	2. Tap on "Configure Face ID".

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 167 of 232

<u>Claim 15</u>	Accused Instrumentalities
	3. Hold the device in portrait mode in front of your face and tap "Let's go".
	4. Make sure your face is inside the frame and slowly move your head until the circle shown is completed. If you can't move your head, tap on "Options for operating aids".
	5. After performing the first Face ID scan, tap "Next".
	6. Again, slowly describe a circle with your head until it is completed.
	7. Tap "Done."
	(https://support.apple.com/en-us/HT208109)
	The biometric signature of a single face is thus determined by two successive Face ID scans, each of which receives a series of entries of the biometric signal (compare steps 4. and 6. above).
	To register a second face, the iPhone offers a corresponding option in its settings. If the user selects the option "Set up an alternative appearance" as shown in the figure below on https://www.macworld.co.uk/how-to/second-face-id-3803421/, a second face is registered by the iPhone in
	the same way as the first face.

.

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 168 of 232

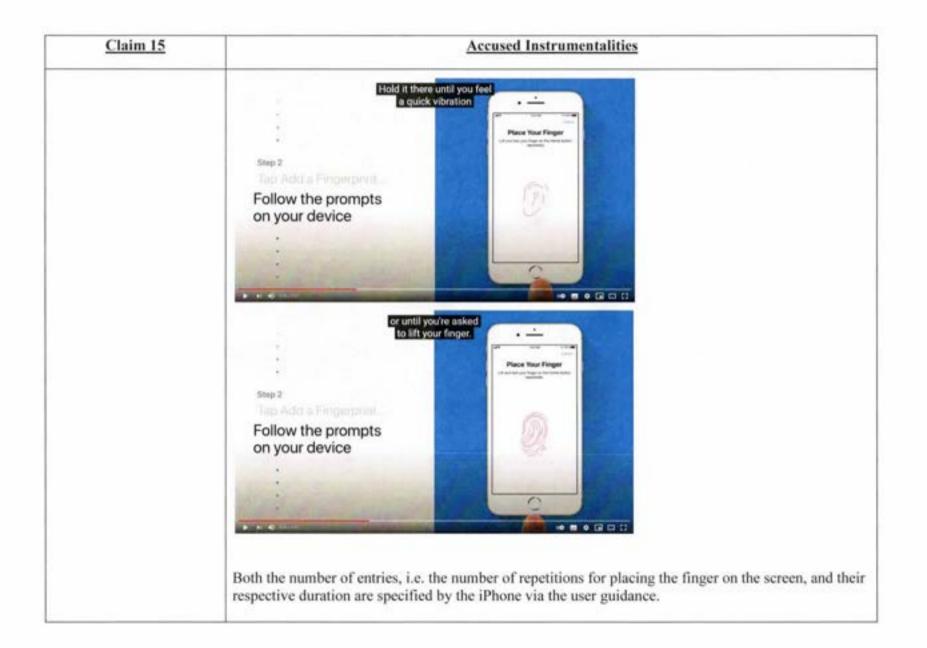
Claim 15	Accused Instrumentalities
	K Settimer Face ID & Pasacode
	VOIL FACE ED FOR
	Phone Unlock
	Ture App Store
	Accil
	Passwo udoFili
	Other Apt 4 Jonn 1
	Where call is a first the control of
	Set Up an Alternative Appearance
	in administrative provinces and advertising from you losse. Factor Of part representate advertually beginner within
	Pesset Faces (D)
	ATTRACTOR
	Require Attention for Face ID
	The series of entries of the biometric signal is identified on the iPhone by both the number and
	duration of each such entry.
	Touch ID
	According to step 5 of the instructions https://support.apple.com/en-us/HT201371, for the enrollment
	of a single finger, the user has to repeatedly place the respective finger on the sensor and thus a number
	of entries in a row predetermined via the user guidance are captured by the iPhone. Each one of the
	entries must also be of a predetermined duration given to the user via the iPhone display, i.e. the user's
	finger must remain on the sensor for a predetermined duration for each entry of the biometric signal in
	order to capture the biometric signal during this time.

Claim 15	Accused Instrumentalities
	Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone and iPad.
	Set up Touch ID
	<ul> <li>4. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</li> </ul>
	B et AM 2005. Control
	Place Your Finger Lift and rest your inger on the Home button repeatedly.
	5. Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.
	6. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you did during the first scan.
	(https://support.apple.com/en-us/HT201371)

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 170 of 232

<u>Claim 15</u>	Accused Instrumentalities
	After placing a finger on the home button, a fingerprint appears on the display with red progress bars spreading along some of the papillary bars until the capture of the biometric entry in question is complete:
	Garcel Place Your Finger
	Lift and rest your imper on the Home button reparts dy.
	When the required duration is reached, the iPhone vibrates after an entry of the biometric signal is received or it issues a prompt to the user to lift the finger. The user then lifts the finger in question and
	replaces the same finger so that the iPhone receives a series of biometric signal entries of sufficient duration for that finger. The process is repeated for the same finger for as long as required according to the iPhone's user guidance. This is shown in the Apple You Tube video (32) How to set up Touch ID on your iPhone or iPad -
	Apple Support - YouTube (https://www.youtube.com/watch?v=xTZ2LALWZlg):

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 171 of 232



# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 172 of 232

Claim 15	Accused Instrumentalities
	Face ID The user moves his face in front of the camera to strike different poses, and the camera system with image sensor continuously captures a large number of biometric entries, i.e. here the 2D images with depth information, in a row.
	"This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)
	The sufficient duration of an entry for a pose, i.e. an angular position of the head specified via the user interface of the iPhone, is indicated to the user by the transformation of a gray line into a green line:
	Means your hand showly to gaugedets the parties.
	(Individual images taken from: https://support.apple.com/en-us/HT208109)
5d2. mapping said series to an instruction; and	The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.

ASSA ABLOY Ex. 1021 - Page 171 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 173 of 232

<u>Claim 15</u>	Accused Instrumentalities
	More specifically, the Secure Enclave of the iPhone contains means to assign the received row to an instruction: The Secure Enclave, after receiving the full set of entries of the biometric signal, assigns this set to an instruction for processing, encrypting and storing the biometric signature ("Touch ID and Face ID template data").
	"The sensor captures the biometric image and securely transmits it to the Secure Enclave. During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Ex. A, Apple Platform Security, at 19.)
	To carry out this instruction, the Secure Enclave has its own processor: "The Secure Enclave Processor provides the main computing power for the Secure Enclave." ( <i>Id.</i> , at 10.)
	Touch ID
	The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.
	"The analysis uses subdermal ridge flow angle mapping, a lossy process that discards "finger minutiae data" that would be required to reconstruct the user's actual fingerprint. During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches, but without any identity information." ( <i>Id.</i> , at 19.)
	<b>Face ID</b> The instruction involves the transformation of the set of entries of the biometric signal captured via the Face ID scans into a mathematical representation, i.e. the biometric signature of the face in question by the Secure Neural Engine of the Secure Enclave, as well as its encryption and storage.

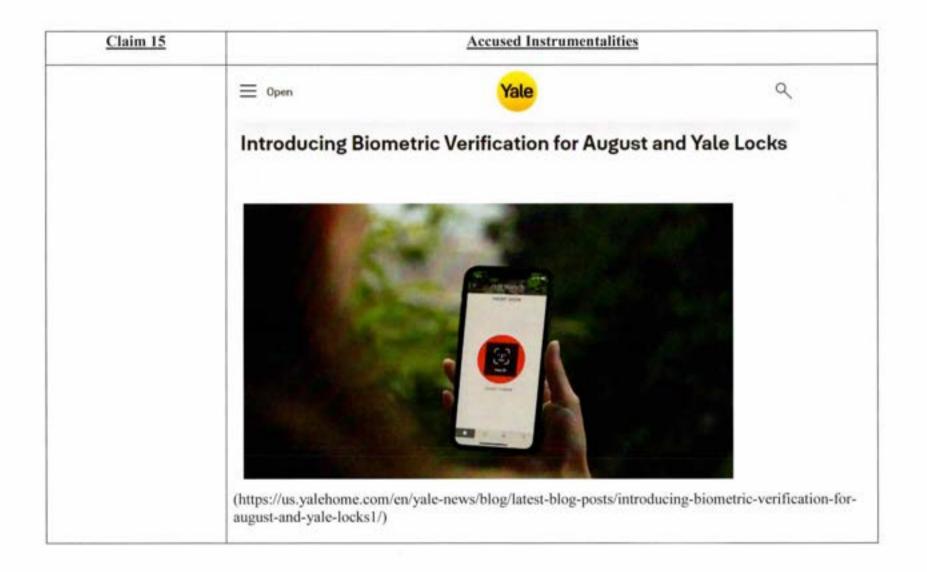
# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 174 of 232

<u>Claim 15</u>	Accused Instrumentalities
	"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses. " ( <i>Id.</i> , at 20.)
	"Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device. It's not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:
	<ul> <li>The mathematical representations of a user's face calculated during enrollment</li> <li>"</li> </ul>
	( <i>Id.</i> , at 23.)
15d3. populating the data base according to the instruction,	The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.
	More specifically, the Secure Enclave stores the biometric signature, i.e. the encrypted mathematical representation of the fingerprint or face, in the database 105, i.e. the "secure nonvolatile storage":
	"The secure nonvolatile storage is used for all anti-replay services in the Secure Enclave. Anti-replay services on the Secure Enclave are used for revocation of data over events that mark anti-replay boundaries including, but not limited to, the following:
	<ul> <li></li> <li>Adding or removing a Touch ID fingerprint or Face ID face".</li> <li>(Ex. A, Apple Platform Security, at 16.)</li> </ul>
	"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." ( <i>Id.</i> , at 19.)

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 175 of 232

Claim 15	Accused Instrumentalities
	Touch ID         "During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches"         (Id.)         Face ID
	<ul> <li>The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:</li> <li>The mathematical representations of a user's face calculated during enrollment". (<i>Id.</i>, at 23.)</li> </ul>
wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.	The Accused Instrumentalities are configured to provide access to the controlled item, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.         More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.
	"When the "Secure Remote Access" feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it." (https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for- august-and-yale-locks1/)

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 176 of 232



ASSA ABLOY Ex. 1021 - Page 175 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 177 of 232



ASSA ABLOY Ex. 1021 - Page 176 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

<u>Claim 16</u>	Accused Instrumentalities
16. A transmitter sub- system for operating in a system for providing secure access to a controlled item, wherein the transmitter sub-system comprises:	To the extent that the preamble is deemed to be a limitation, the Accused Instrumentalities include a transmitter sub-system for operating in a system for providing secure access to a controlled item in accordance with this claim.
16a. a biometric sensor capable of receiving a biometric signal;	The Accused Instrumentalities include a biometric sensor configured to receive a biometric signal. More specifically, the iPhone has at least one biometric sensor for capturing a fingerprint or a face (Touch ID and/or Face ID), namely a Touch ID sensor and a camera system with image sensor, respectively. Touch ID
	<ul> <li>"Apple devices with a Touch ID sensor can be unlocked using a fingerprint."</li> <li>(Ex. A, Apple Platform Security, at 19.)</li> <li>"Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the sensor continuing to expand the fingerprint map as additional overlapping nodes are identified with each use."</li> <li>(<i>Id.</i>)</li> <li>"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave."</li> <li>(<i>Id.</i>)</li> <li>The biometric sensor for Touch ID is located below the home button:</li> </ul>

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 179 of 232

Claim 16	Accused Instrumentalities
	"The Home button is a stack of different materials, capped with a sapphire crystal lens. The surrounding stainless-steel ring works as a ground and detects the user's finger. This action activates a capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors." (https://appleinsider.com/inside/touch-id)
	Biometric sensor 121 "Where is the Touch ID sensor located?
	The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.
	(https://support.apple.com/en-us/HT201371)
	The image sensor captures an 88-by-88-pixel, 500 PPI raster scan:
	"The 88-by-88-pixel, 500-ppi raster scan is temporarily stored in encrypted memory within the Secur Enclave while being vectorized for analysis, and then it's discarded. The analysis utilizes subdermal

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 180 of 232

Claim 16	Accused Instrumentalities					
	ridge flow angle mapping, which is a lossy process that discards minutia data that would be required to reconstruct the user's actual fingerprint. The resulting map of nodes is stored without any identity information in an encrypted format that can only be read by the Secure Enclave, and is never sent to Apple or backed up to iCloud or iTunes. " (Ex. C, iOS Security white paper, at 8.)					
	Face ID					
	The biometric sensor for facial biometrics is a camera system (" <b>TrueDepth</b> camera <b>system</b> ") with an image sensor.					
	"With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face. " (Ex. A, Apple Platform Security, at 20.)					
	To receive a biometric signal, the camera system with image sensor reads over 30,000 infrared points to capture depth information along with a two-dimensional infrared image.					
	"After the TrueDepth camera confirms the presence of an attentive face, it projects and <b>reads over</b> <b>30,000 infrared dots to form a depth map of the face along with a 2D infrared image</b> . This data is used to <b>create a sequence of 2D images and depth maps</b> , which are digitally signed and sent to the Secure Enclave. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." ( <i>Id.</i> )					

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 181 of 232

<u>Claim 16</u>	Accused Instrumentalities					
	The camera system includes a biometric image sensor, namely a "CMOS image" sensor from Sony, to perform facial biometrics:					
	Structured light receiver Moode Hon-nel, Dharp CM-25 areas and rest 4MMS STM CSI (and second and the Tong Huang CSI (and second and the Tong Huang State Wate Stat	Antonio antonio Antonio Antonio Antonio Antonio Antonio Antonio Antonio Antonio		Econticamera Nove Handak Creek Orlin Color anos antor 1995 Sery Conset Largan Ornas Largan Artis	Constant of Long Andrews Model Constant and the constant Constant and the constant Constant and the constant Constant and the constant Constant and the constant of surface Name of Constant and surface Name of	
			Active alignment		Active algoment equipment.	
	(https://appleinside report)	er.com/articles/1	7/09/09/inner-wo	rkings-of-apples-f	ace-id-camera-detailed-in-	
6b. a controller capable of matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute; and	The Accused Instrumentalities include a transmitter controller configured to emit a secure access signal conveying information dependent upon said accessibility attribute.         More specifically, the iPhone's System on Chip (SOC), i.e. the Secure Enclave with its Secure Enclave Processor (SEP) or a Secure Neural Engine contained therein, is a means (103) to check a match of the biometric signal with elements of the biometric signature database.					

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 182 of 232

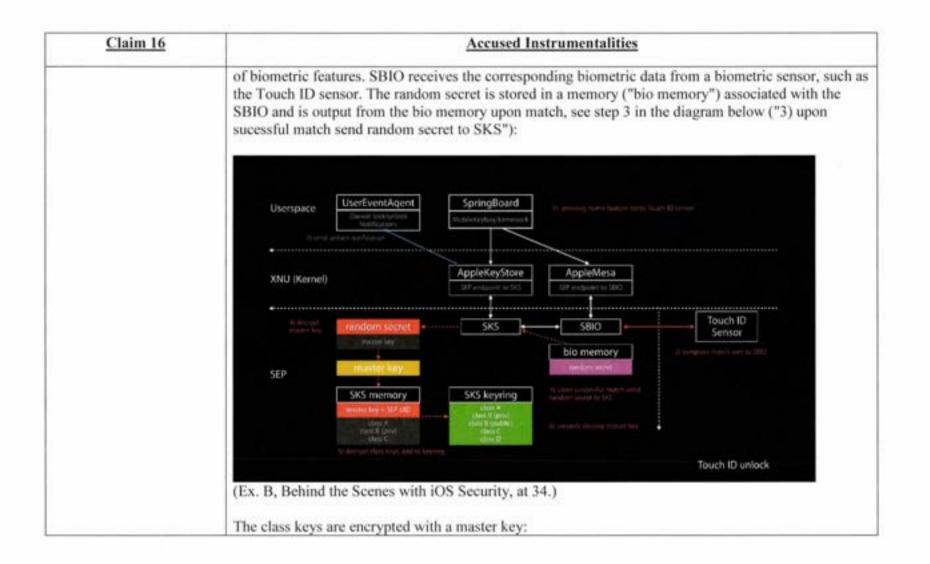
Claim 16	Accused Instrumentalities
	"The Secure Enclave is a system on chip (SoC) that is included on all recent iPhone, devices" (Ex. A, Apple Platform Security, at 7.)
	"During <b>matching</b> , the Secure Enclave <b>compares</b> incoming data from the biometric sensor against the stored templates <b>to determine whether to unlock the device</b> or respond that a match is valid (for Apple Pay, in-app, and other uses of Touch ID and Face ID). " ( <i>Id.</i> , at 19.)
	The biometric signal received from the biometric sensor ("incoming data from the biometric sensor") is thus checked by the Secure Enclave and its SEP with the elements of the database of biometric signatures 105, i.e. the "stored templates", for the presence of a match.
	For Touch ID, the Secure Enclave match verification is performed as follows:
	"The Secure Enclave is responsible for processing fingerprint data from the Touch ID sensor, determining if there is a match against registered fingerprints, and then enabling access or purchases on behalf of the user"
	(Ex. C, iOS Security white paper, at 7.)
	"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches" (Ex. A, Apple Platform Security, at 19.)
	"Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. " (https://support.apple.com/en-us/HT204587)
	"Touch ID can read multiple fingerprints and recognize fingerprints at any orientation of the finger. The system then creates a mathematical representation of your fingerprint and compares it to the registered fingerprint data to determine a match and unlock your device."

<u>Claim 16</u>	Accused Instrumentalities
	(https://support.apple.com/de-de/HT204587)
	For <b>Face ID</b> , the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:
	"Face ID uses neural networks for determining attention, <b>matching</b> , and antispoofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)
	"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." ( <i>Id.</i> ).
	"Facial matching security
	Facial matching is performed within the Secure Enclave using neural networks trained specifically for that purpose Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device." ( <i>Id.</i> at 23.)
	When the Secure Enclave, or more precisely the Touch ID or Face ID subsystem within the Secure Enclave, has determined that a match exists, an accessibility attribute is issued by the corresponding Touch ID or Face ID subsystem. This Touch ID or Face ID subsystem is also referred to as the SBIO. The accessibility attribute confirms that there is a match and that the iPhone is to be unlocked (" determine whether to unlock the device").
	This confirmation of the match is signaled by the SBIO by issuing a random secret to which only the Touch ID or Face ID subsystem within the Secure Enclave has access:

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 184 of 232

Claim 16	Accused Instrumentalities
	"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device []." ( <i>Id.</i> at 19.)
	"Uses for Touch ID and Face ID
	Unlocking a device or user account
	[] keys for the highest class of Data Protection-which are held in the Secure Enclave [].
	With Touch ID or Face ID enabled, the keys aren't discarded when the device or account locks; instead, they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the Secure Enclave. When a user attempts to unlock the device or account, if the device detects a successful match, it provides the key for unwrapping the Data Protection keys, and the device or account is unlocked. This process provides additional protection by requiring cooperation between the Data Protection and Touch ID or Face ID subsystems to unlock the device."
	( <i>Id.</i> at 24.)
	"The class key is protected with the hardware UID and, for some classes, the user's passcode." ( <i>Id.</i> at 85.)
	"Complete Protection
	<i>(NSFileProtectionComplete):</i> The class key is protected with a key derived from the user passcode or password and the device UID. Shortly after the user locks a device (10 seconds, if the Require Password setting is Immediately), the decrypted class key is discarded, <b>rendering all data in this class inaccessible until the user</b> enters the passcode again or <b>unlocks</b> (logs in to) <b>the device using Touch ID or Face ID.</b> "
	( <i>Id.</i> at 86.)
	The Touch ID or Face ID subsystem within the Secure Enclave is the SBIO shown below. SBIO is an application that runs within the Secure Enclave on the SEP and is responsible for checking the match

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 185 of 232



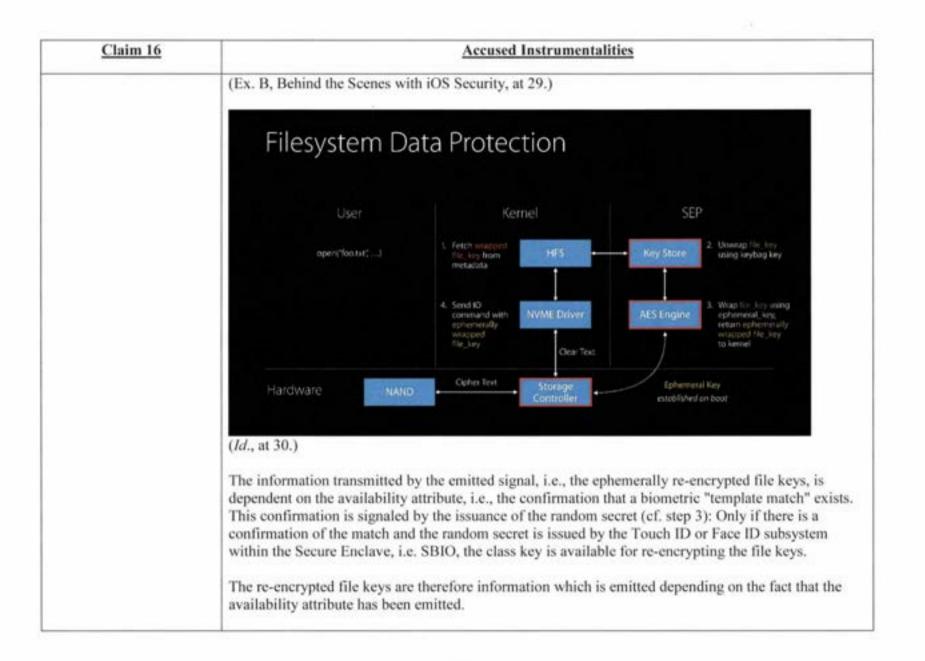
ASSA ABLOY Ex. 1021 - Page 184 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

Claim 16	Accused Instrumentalities
	User Keybags
	Background
	Sets of keys generated for each user to protect their data at rest
	Keys wrapped by master key derived from user passcode and SEP UID
	After 10 incorrect passcode entries, SEP will not process any further attempts
	Different policy associated with each keybag key—Usage, availability
	(Id., at 25.)
	The random secret is issued to SKS. SKS is a Secure Key Service application which is located within the Secure Enclave on the SEP and is responsible for decrypting class keys. The random secret provided by SBIO is used to decrypt a master key ("4) decrypt master key"). The master key is concatenated with the UID of the SEP and thus class keys are decrypted and added to the SKS keyring ("5) decrypt class keys, add to keyring") for further use by the Secure Enclave. The decrypted class keys include, for example, the class key of class A.
16c. a transmitter capable of emitting a secure access signal conveying said	The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.
information dependent upon said accessibility	For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys:
attribute;	"sepOS can then use the ephemeral wrapping key to wrap file keys for use by the Application Processor file-system driver. When the file-system driver reads or writes a file, it sends the wrapped key to the AES Engine."

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 187 of 232

Claim 16	Accused Instrumentalities
	(Ex. A, Apple Platform Security, at 14.)
	"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. [] When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." ( <i>Id.</i> at 85.)
	The signal with the ephemerally re-encrypted file keys is a secure signal because it comes from the Secure Enclave and thus from a secure environment. Furthermore, the signal is secure because the transmitted information is encrypted. The emitted file keys are encrypted with the ephemeral key:
	"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. At startup, the Secure Enclave negotiates an ephemeral key with the AES Engine. When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." ( <i>Id.</i> )
	Filesystem Data Protection
	Overview
	File blocks are encrypted using AES-XTS with 128-bit keys
	Each file on the user partition is encrypted using a unique random key chosen by SE
	Raw file keys are never exposed to the AP
	Wrapped with a key from the user keybag for long-term storage
	<ul> <li>Wrapped with an ephemeral key while in use, bound to boot session</li> </ul>

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 188 of 232



Claim 16	Accused Instrumentalities
16d. wherein the controller is further capable of:	The Accused Instrumentalities include a controller that has capabilities as set forth in elements 16d1, 16d2, and 16d3 below.
16d1. receiving a series of entries of the biometric signal, said series being	The Accused Instrumentalities include a transmitter sub-system controller configured to receive a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry.
characterised according to at least one of the number of said entries and a duration of each said	More specifically, the Secure Enclave of the iPhone with the Secure Enclave Processor forms the means for receiving a series of entries of the biometric signal.
entry;	"Apple's biometric security architecture relies on a strict separation of responsibilities between the biometric sensor and the Secure Enclave, and a secure connection between the two. The sensor captures the biometric image and securely transmits it to the Secure Enclave." (Ex. A, Apple Platform Security, at 19.)
	Touch ID
	When a finger is placed on the biometric sensor, the finger is scanned and the corresponding biometric signal entry is received by the Secure Enclave.
	"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave." ( <i>Id.</i> )
	To enroll a fingerprint in the database, the iPhone's fingerprint sensor records an entry of a biometric signal when the user places his finger on the sensor. This is done multiple times, resulting in a series of entries of such biometric signals.
	Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone.

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 190 of 232

Claim 16	Accused Instrumentalities
	Set up Touch ID
	Before you can set up Touch ID, you must first create a <u>code</u> for your device,* then follow these steps: 25. Make sure the Touch ID sensor and your finger are clean and dry.
	26. Tap Settings > Touch ID & Code, and then enter your code.
	<ol> <li>Tap "Add fingerprint" and hold the device as you normally would when touching the Touch ID sensor.</li> </ol>
	28. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.           Place Your Finger
	<ol> <li>Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.</li> </ol>

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 191 of 232

Claim 16	Accused Instrumentalities
	30. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you would during the first scan."
	(https://support.apple.com/en-us/HT201371)
	Accordingly, the user is prompted to place his finger on the sensor several times, in particular in accordance with step 5. Each time the finger is placed on the sensor, a corresponding biometric entry is generated, i.e. a series of such entries. All these entries, which result from placing the same finger on the sensor, form a series.
	Face ID
	The means for receiving a series of entries of the biometric signal includes a Secure Neural Engine, which is protected by the Secure Enclave. The Secure Neural Engine transforms the series of entries of the biometric signal received by the Secure Enclave into a biometric signature ("mathematical representation").
	"After the TrueDepth camera confirms the presence of an attentive face, it projects and reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image. This data is used to create a sequence of 2D images and depth maps, which are digitally signed and sent to the Secure Enclave. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)
	Each entry of the biometric signal thus contains a two-dimensional infrared image with 30,000 infrared points for capturing depth information. By continuously capturing such infrared images into a Face ID scan while the user moves his head into different poses, a series of entries of the biometric signal

### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 192 of 232

<u>Claim 16</u>	Accused Instrumentalities
	results. Two such Face ID scans are required to generate a biometric signature of a single face, so that two series of entries of the biometric signal are received accordingly.
	Using Face ID on iPhone
	1. Tap Settings > Face ID & Code. Enter your code when prompted.
	2. Tap on "Configure Face ID".
	3. Hold the device in portrait mode in front of your face and tap "Let's go".
	4. Make sure your face is inside the frame and slowly move your head until the circle shown is completed. If you can't move your head, tap on "Options for operating aids".
	5. After performing the first Face ID scan, tap "Next".
	6. Again, slowly describe a circle with your head until it is completed.
	7. Tap "Done."
	(https://support.apple.com/en-us/HT208109)
	The biometric signature of a single face is thus determined by two successive Face ID scans, each of which receives a series of entries of the biometric signal (compare steps 4. and 6. above).
	To register a second face, the iPhone offers a corresponding option in its settings. If the user selects the option "Set up an alternative appearance" as shown in the figure below on https://www.macworld.co.uk/how-to/second-face-id-3803421/, a second face is registered by the iPhone in the same way as the first face.

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 193 of 232

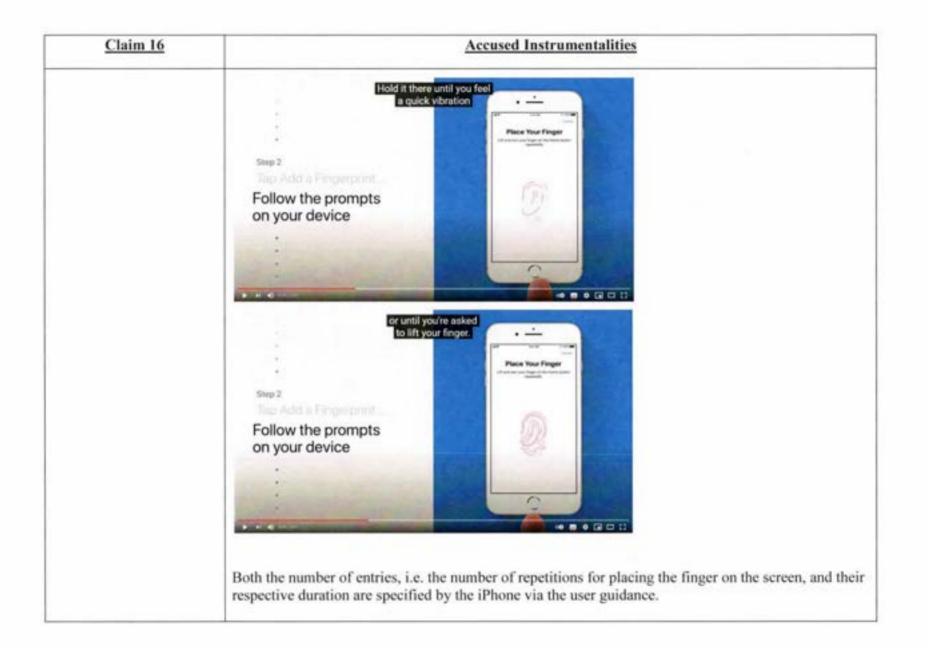
Claim 16	Accused Instrumentalities
	Significant Face ID & Passcode
	Leo .
	LISE FACE ID FOR
	Phone Unlock C
	Apple - U
	Passed uddFill
	Final and the state of the stat
	Instruction of an analysis and an analysis of a page and an analysis of a page and a
	Set Up an Alternative Appearance
	In addition to contractually learning have plus load. Facel 20 Sam missione an administration topological contract
	Reset Face ID
	Require Attention for Face ID
	Require Admittor for Face D
	The series of entries of the biometric signal is identified on the iPhone by both the number and duration of each such entry.
	Touch ID
	According to step 5 of the instructions https://support.apple.com/en-us/HT201371, for the enrollment
	of a single finger, the user has to repeatedly place the respective finger on the sensor and thus a number
	of entries in a row predetermined via the user guidance are captured by the iPhone. Each one of the
	entries must also be of a predetermined duration given to the user via the iPhone display, i.e. the user's
	finger must remain on the sensor for a predetermined duration for each entry of the biometric signal in
	order to capture the biometric signal during this time.

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 194 of 232

Claim 16	Accused Instrumentalities
	Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone and iPad.
	Set up Touch ID
	<ol> <li>Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</li> </ol>
	Place Your Finger
	<ol> <li>Continue by raising and slowly lowering your finger over and over again, changing the position or your finger just a tiny bit at a time.</li> </ol>
	6. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you did during the first scan.
	(https://support.apple.com/en-us/HT201371)

Claim 16	Accused Instrumentalities
	After placing a finger on the home button, a fingerprint appears on the display with red progress bars spreading along some of the papillary bars until the capture of the biometric entry in question is complete:
	When the required duration is reached, the iPhone vibrates after an entry of the biometric signal is received or it issues a prompt to the user to lift the finger. The user then lifts the finger in question and replaces the same finger so that the iPhone receives a series of biometric signal entries of sufficient duration for that finger. The process is repeated for the same finger for as long as required according to the iPhone's user guidance. This is shown in the Apple You Tube video (32) How to set up Touch ID on your iPhone or iPad - Apple Support - YouTube (https://www.youtube.com/watch?v=xTZ2LALWZlg):

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 196 of 232



# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 197 of 232

Claim 16	Accused Instrumentalities
	Face ID The user moves his face in front of the camera to strike different poses, and the camera system with image sensor continuously captures a large number of biometric entries, i.e. here the 2D images with depth information, in a row.
	"This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)
	The sufficient duration of an entry for a pose, i.e. an angular position of the head specified via the user interface of the iPhone, is indicated to the user by the transformation of a gray line into a green line:
	Merry prior hand showly to complete The circle. Merry prior hand showly to complete The circle.
d2. mapping said series	(Individual images taken from: https://support.apple.com/en-us/HT208109)
to an instruction; and	The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 198 of 232

<u>Claim 16</u>	Accused Instrumentalities
	More specifically, the Secure Enclave of the iPhone contains means to assign the received row to an instruction: The Secure Enclave, after receiving the full set of entries of the biometric signal, assigns this set to an instruction for processing, encrypting and storing the biometric signature ("Touch ID and Face ID template data").
	"The sensor captures the biometric image and securely transmits it to the Secure Enclave. During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Ex. A, Apple Platform Security, at 19.)
	To carry out this instruction, the Secure Enclave has its own processor: "The Secure Enclave Processor provides the main computing power for the Secure Enclave." ( <i>Id.</i> , at 10.)
	Touch ID
	The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.
	"The analysis uses subdermal ridge flow angle mapping, a lossy process that discards "finger minutiae data" that would be required to reconstruct the user's actual fingerprint. During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches, but without any identity information." ( <i>Id.</i> , at 19.)
	<b>Face ID</b> The instruction involves the transformation of the set of entries of the biometric signal captured via the Face ID scans into a mathematical representation, i.e. the biometric signature of the face in question by the Secure Neural Engine of the Secure Enclave, as well as its encryption and storage.

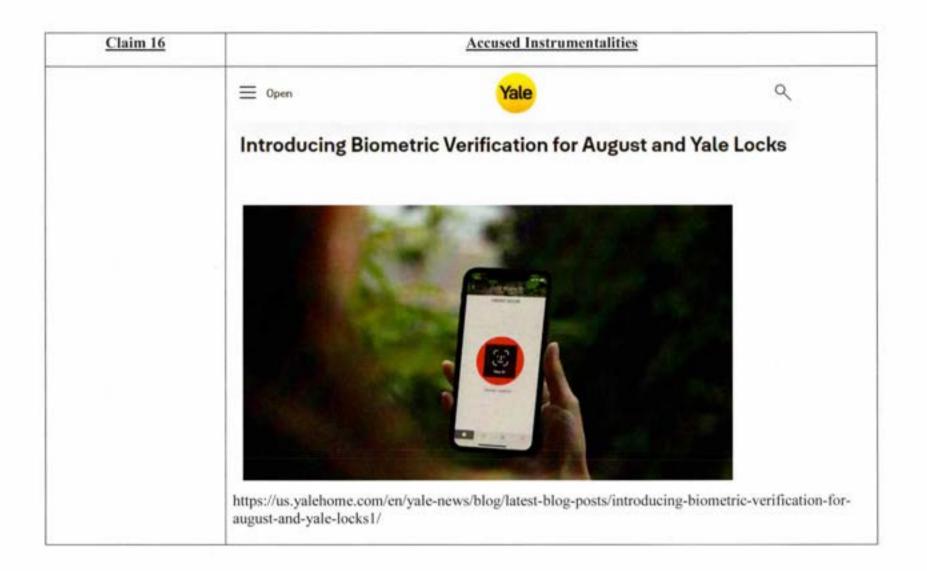
<u>Claim 16</u>	Accused Instrumentalities
	"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses. " ( <i>Id.</i> , at 20.)
	"Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device. It's not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:
	The mathematical representations of a user's face calculated during enrollment    "     ( <i>Id.</i> , at 23.)
16d3. populating the database according to the instruction	The Accused Instrumentalities include a transmitter sub-system controller configured to populate the database according to the instruction.
instruction,	More specifically, the Secure Enclave stores the biometric signature, i.e. the encrypted mathematical representation of the fingerprint or face, in the database 105, i.e. the "secure nonvolatile storage":
	"The secure nonvolatile storage is used for all anti-replay services in the Secure Enclave. Anti-replay services on the Secure Enclave are used for revocation of data over events that mark anti-replay boundaries including, but not limited to, the following:
	<ul> <li></li> <li>Adding or removing a Touch ID fingerprint or Face ID face". (Ex. A, Apple Platform Security, at 16.)</li> </ul>
	"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." ( <i>Id.</i> , at 19.)

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 200 of 232

Claim 16	Accused Instrumentalities
	Touch ID         "During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches"         (Id.)         Face ID
	<ul> <li>The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:</li> <li>The mathematical representations of a user's face calculated during enrollment".</li> <li>(<i>Id.</i>, at 23.)</li> </ul>
wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.	<ul> <li>The Accused Instrumentalities include a controller capable of: populating the database according to the instruction, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.</li> <li>More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.</li> </ul>
	"When the "Secure Remote Access" feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it." https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for- august-and-yale-locks1/

ASSA ABLOY Ex. 1021 - Page 199 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 201 of 232

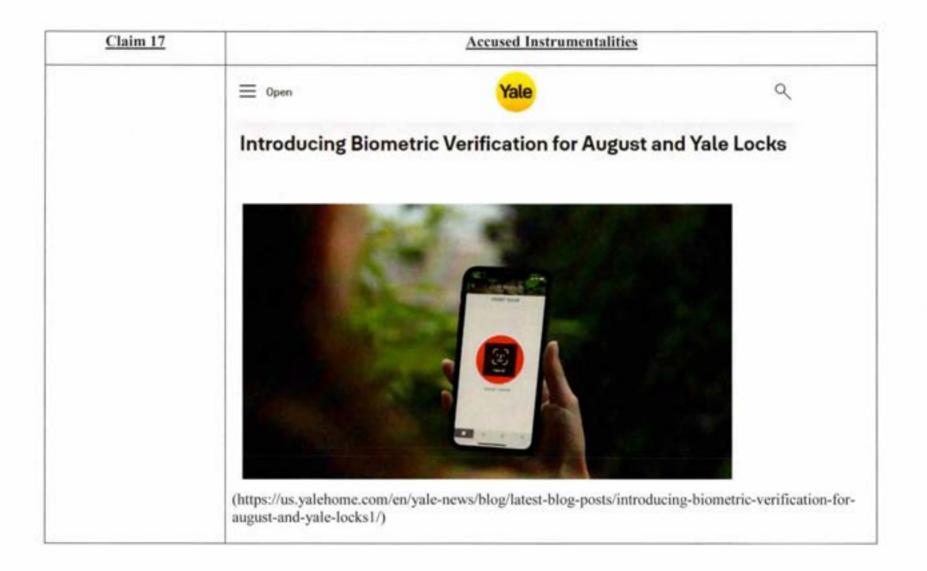


#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 202 of 232

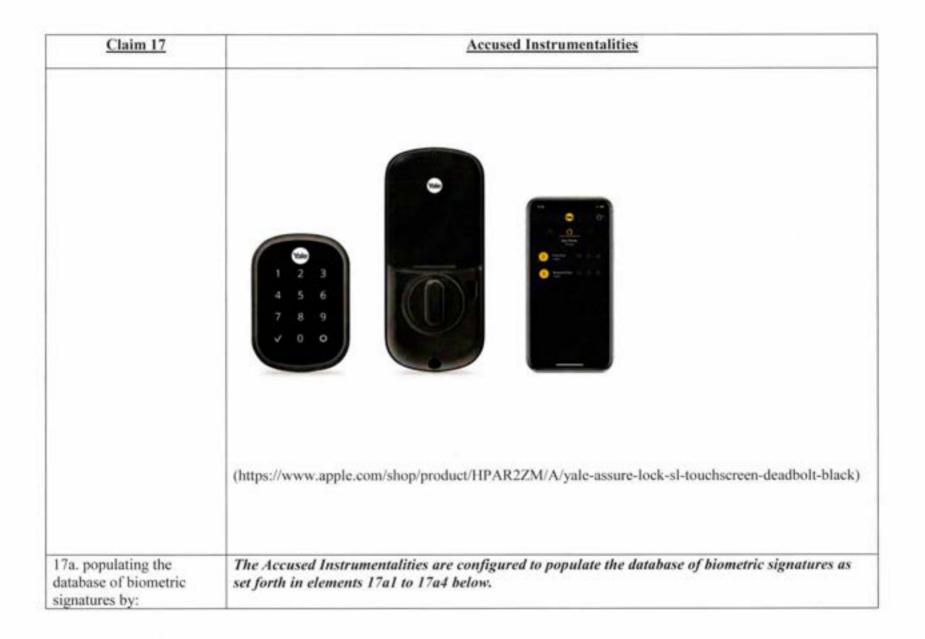


<u>Claim 17</u>	Accused Instrumentalities
Claim 17 17. A method for providing secure access to a controlled item in a system comprising a database of biometric signatures, a transmitter sub-system comprising a biometric sensor capable of receiving a biometric signal, and a transmitter capable of emitting a secure access signal capable of granting access to the controlled item, and a receiver sub-system comprising a receiver sub- system controller capable of receiving the transmitted secure access signal, and providing conditional access to the controlled item dependent	Accused Instrumentalities           To the extent that the preamble is deemed to be a limitation, the Accused Instrumentalities are configured to use a method in accordance with this claim.           More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID.           "When the "Secure Remote Access" feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it." (https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/)

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 204 of 232



#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 205 of 232



<u>Claim 17</u>	Accused Instrumentalities
17a1. receiving a series of entries of the biometric signal;	The Accused Instrumentalities are configured to populate the database of biometric signatures by: receiving a series of entries of the biometric signal.
	More specifically, the Secure Enclave of the iPhone with the Secure Enclave Processor forms the means for receiving a series of entries of the biometric signal.
	"Apple's biometric security architecture relies on a strict separation of responsibilities between the biometric sensor and the Secure Enclave, and a secure connection between the two. The sensor captures the biometric image and securely transmits it to the Secure Enclave." (Ex. A, Apple Platform Security, at 19.)
	Touch ID
	When a finger is placed on the biometric sensor, the finger is scanned and the corresponding biometric signal entry is received by the Secure Enclave.
	"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave."
	(Ex. A, Apple Platform Security, at 19.) To enroll a fingerprint in the database, the iPhone's fingerprint sensor records an entry of a biometric signal when the user places his finger on the sensor. This is done multiple times, resulting in a series of entries of such biometric signals.
	Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone and iPad here - Apple Support ; https://support.apple.com/en-us/HT201371
	literally described as follows:
	Set up Touch ID

ASSA ABLOY Ex. 1021 - Page 205 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 207 of 232

<u>Claim 17</u>	Accused Instrumentalities
	Before you can set up Touch ID, you must first create a code for your device,* then follow these steps: 1. Make sure the Touch ID sensor and your finger are clean and dry.
	2. Tap Settings > Touch ID & Code, and then enter your code.
	3. Tap "Add fingerprint" and hold the device as you normally would when touching the Touch ID sensor.
	<ol> <li>Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until you feel a quick vibration or are prompted to lift your finger.</li> </ol>
	Carte  Place Your Finger  Ut and met your finger on the Home button repeatedly:
	<ol> <li>Continue by raising and slowly lowering your finger over and over again, changing the position of your finger just a tiny bit at a time.</li> </ol>
	<ul> <li>6. The next screen will ask you to change your finger position. Hold your device as you normally would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you would during the first scan."</li> </ul>

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 208 of 232

Claim 17	Accused Instrumentalities
	Accordingly, the user is prompted to place his finger on the sensor several times, in particular in accordance with step 5. Each time the finger is placed on the sensor, a corresponding biometric entry is generated, i.e. a series of such entries. All these entries, which result from placing the same finger on the sensor, form a series.
	Face ID
	The means for receiving a series of entries of the biometric signal includes a Secure Neural Engine, which is protected by the Secure Enclave. The Secure Neural Engine transforms the series of entries of the biometric signal received by the Secure Enclave into a biometric signature ("mathematical representation").
	"After the TrueDepth camera confirms the presence of an attentive face, it projects and reads over 30,000 infrared dots to form a depth map of the face along with a 2D infrared image. This data is used to create a sequence of 2D images and depth maps, which are digitally signed and sent to the Secure Enclave. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)
	Each entry of the biometric signal thus contains a two-dimensional infrared image with 30,000 infrared points for capturing depth information. By continuously capturing such infrared images into a Face ID scan while the user moves his head into different poses, a series of entries of the biometric signal results. Two such Face ID scans are required to generate a biometric signature of a single face, so that two series of entries of the biometric signal are received accordingly.
	Under Using Face ID on iPhone or iPad Pro - Apple Support; <u>https://support.apple.com/en-us/HT208109</u> , the creation of a set of entries is described as follows:

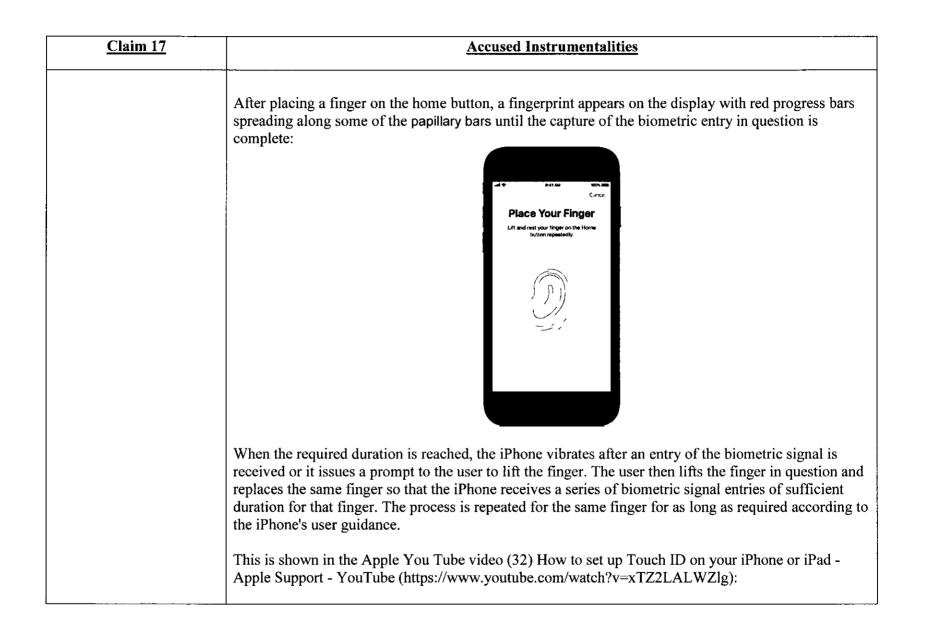
<u>Claim 17</u>	Accused Instrumentalities
	Configure Face ID
	Before configuring Face ID, make sure that neither the TrueDepth camera nor your face are covered by anything
	Follow the steps below to configure Face ID:
	1. Tap Settings > Face ID & Code. Enter your code when prompted.
	2. Tap on "Configure Face ID".
	3. Hold the device in portrait mode in front of your face and tap "Let's go".
	4. Make sure your face is inside the frame and slowly move your head until the circle shown is completed. If you can't move your head, tap on "Options for operating aids".
	5. After performing the first Face ID scan, tap "Next".
	6. Again, slowly describe a circle with your head until it is completed.
	7. Tap "Done."
	The biometric signature of a single face is thus determined by two successive Face ID scans, each of which receives a series of entries of the biometric signal (compare steps 4. and 6. above).
	To register a second face, the iPhone offers a corresponding option in its settings. If the user selects the option "Set up an alternative appearance" as shown in the figure below on https://www.macworld.co.uk/how-to/second-face-id-3803421/, a second face is registered by the iPhone in the same way as the first face.

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 210 of 232

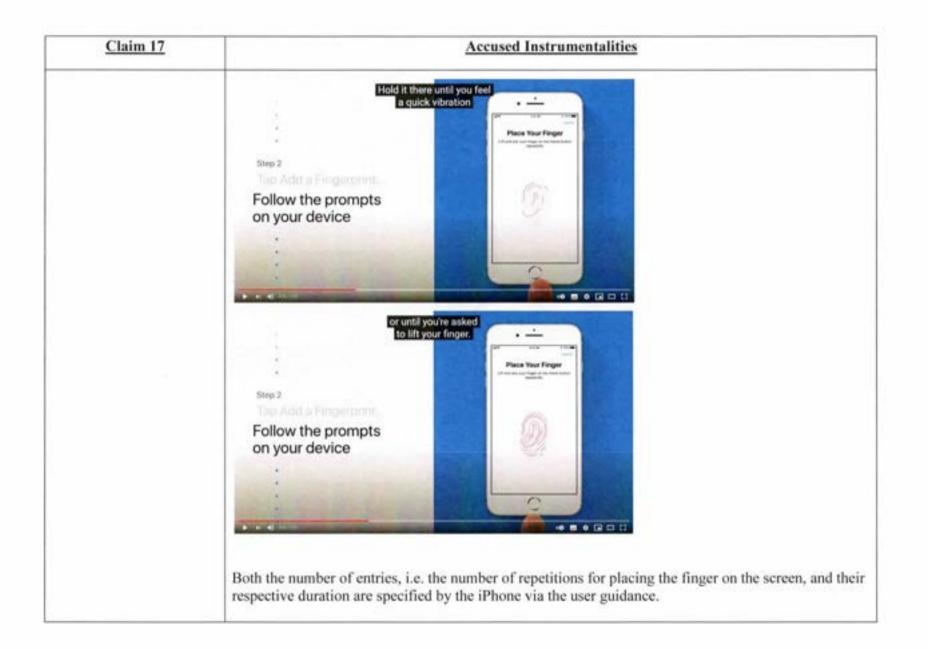
Claim 17	Accused Instrumentalities
	C Setteval Face ID & Passcode
	Phone Unlock
	Turente App Store
	Appl
	Pasuwo udofil
	Other Act 4 Apps
	When a the for an and the present the second to appro- mentation of a for the second to appro- ant comments and the second to appro- te the D-B Presents.
	Set Up an Alternative Appearance
	b) addition to continuously barrong from you tool. Face 3D our recognises at alternative separations.
	Reset Fate D
	ATTENTON
	Require Attention for Face ID
	The series of entries of the biometric signal is identified on the iPhone by both the number and
	duration of each such entry.
	Touch ID
	A sector of the last standard and and and and and and and and and a sector of the sector beauty
	According to step 5 of the instructions https://support.apple.com/en-us/HT201371, for the enrollment
	of a single finger, the user has to repeatedly place the respective finger on the sensor and thus a number
	of entries in a row predetermined via the user guidance are captured by the iPhone. Each one of the
	entries must also be of a predetermined duration given to the user via the iPhone display, i.e. the user's
	finger must remain on the sensor for a predetermined duration for each entry of the biometric signal in
	order to capture the biometric signal during this time.

Claim 17	Accused Instrumentalities
	Receiving a series of entries of the biometric signal by repeatedly placing a finger on the Touch ID sensor will use Touch ID on iPhone and iPad here - Apple Support (https://support.apple.com/en-us/HT201371) literally described as follows:
	<ul> <li>Set up Touch ID</li> <li></li> <li>4. Touch the Touch ID sensor with one finger, but do not press. Keep your finger on the button until</li> </ul>
	you feel a quick vibration or are prompted to lift your finger.
	<ul> <li>5. Continue by raising and slowly lowering your finger over and over again, changing the position of</li> </ul>
	<ul> <li>your finger just a tiny bit at a time.</li> <li>6. The next screen will ask you to change your finger position. Hold your device as you normally</li> </ul>
	would when unlocking it. Touch the Touch ID sensor with the outer edges of your fingertip instead of the middle part as you did during the first scan.

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 212 of 232



#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 213 of 232



# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 214 of 232

Accused Instrumentalities
Face ID The user moves his face in front of the camera to strike different poses, and the camera system with image sensor continuously captures a large number of biometric entries, i.e. here the 2D images with depth information, in a row.
"This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." (Ex. A, Apple Platform Security, at 20.)
The sufficient duration of an entry for a pose, i.e. an angular position of the head specified via the use interface of the iPhone, is indicated to the user by the transformation of a gray line into a green line:
Move your head showly to complete the circle.  Move your head showly to complete the circle.  First Face ID score complete.

<u>Claim 17</u>	Accused Instrumentalities
17a2. determining at least one of the number of said entries and a duration of each said entry;	The Accused instrumentalities are configured to populate the database of biometric signatures by: determining at least one of the number of said entries and a duration of each said entry.
	More specifically, as discussed above, both Face ID and Touch ID require a specific number of entries to enroll a Touch ID or Face ID. The Accused Instrumentalities must determine that the specific number of entries have been input. Likewise, while not necessary for the claim, upon information and belief, the Accused Instrumentalities determine that each input of either facial or fingerprint data is of a sufficient duration. Again, when setting up Touch ID in the Accused Instrumentalities, the users are required to touch the home button with their finger several times for a certain duration. Similarly, the users need to scan their face twice, and each scan requires the users to move their head in a circle for a certain duration for Face ID.
	Touch ID: Register a fingerprint for Apple Touch ID by the user tapping a finger several times on the home button to record the fingerprint data. (https://video.search.yahoo.com/yhs/search?fr=yhs-pty_pty_converter&hsimp=yhs-pty_converter&hspart=pty&p=registering+ fingerprint+apple+touch+id+on+screen+instructions#id=1&vid= 156de65ae06ca453643009fc0ea9cf79&action=click)
	Touch ID: The user's finger must remain on the home button long enough for the data to be recorded. "Touch the Touch ID sensor with your finger, but don't press it. Hold it there until you feel a quick vibration, or until you're asked to lift your finger." "Continue to lift and rest your finger slowly, making small adjustments to the position of your finger each time." (https://support.apple.com/en-au/HT201371)
	Touch ID: "you shouldn't tap too quickly or move your finger around" (https://support.apple.com/en-us/HT207537)
	Face ID: Setting up Face ID requires two scans of the user's face. Each scan asks users to move their head slowly in a circle to register different angles of the user's face. (https://www.imore.com/how-set-face-id-iphone)

<u>Claim 17</u>	Accused Instrumentalities
17a3. mapping said series into an instruction; and	The Accused Instrumentalities include a transmitter sub-system controller configured to map said series into an instruction.
	More specifically, the Secure Enclave of the iPhone contains means to assign the received row to an instruction: The Secure Enclave, after receiving the full set of entries of the biometric signal, assigns this set to an instruction for processing, encrypting and storing the biometric signature ("Touch ID and Face ID template data").
	"The sensor captures the biometric image and securely transmits it to the Secure Enclave. During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." (Ex. A, Apple Platform Security, at 19.)
	To carry out this instruction, the Secure Enclave has its own processor: "The Secure Enclave Processor provides the main computing power for the Secure Enclave." ( <i>Id.</i> , at 10.)
	Touch ID
	The instruction here involves the processing of under-the-skin fingerprint characteristics and their encrypted storage.
	"The analysis uses subdermal ridge flow angle mapping, a lossy process that discards "finger minutiae data" that would be required to reconstruct the user's actual fingerprint. During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches, but without any identity information." ( <i>Id.</i> , at 19.)
	Face ID

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 217 of 232

<u>Claim 17</u>	Accused Instrumentalities
	The instruction involves the transformation of the set of entries of the biometric signal captured via the Face ID scans into a mathematical representation, i.e. the biometric signature of the face in question by the Secure Neural Engine of the Secure Enclave, as well as its encryption and storage.
	"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses. " ( <i>Id.</i> , at 20.)
	<ul> <li>"Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device. It's not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:</li> <li>The mathematical representations of a user's face calculated during enrollment</li> <li>"</li> </ul>
17a4. populating the	( <i>Id.</i> , at 23.) The Accused Instrumentalities include a transmitter sub-system controller configured to populate
database according to the	the database according to the instruction.
instruction;	More specifically, the Secure Enclave stores the biometric signature, i.e. the encrypted mathematical representation of the fingerprint or face, in the database 105, i.e. the "secure nonvolatile storage":
	"The secure nonvolatile storage is used for all anti-replay services in the Secure Enclave. Anti-replay services on the Secure Enclave are used for revocation of data over events that mark anti-replay boundaries including, but not limited to, the following:
	•
	<ul> <li>Adding or removing a Touch ID fingerprint or Face ID face".</li> <li>(Ex. A, Apple Platform Security, at 16.)</li> </ul>

Claim 17	Accused Instrumentalities		
	"During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." ( <i>Id.</i> , at 19.)		
	Touch ID		
	"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches" ( <i>Id.</i> )		
	Face ID		
	The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:		
	• The mathematical representations of a user's face calculated during enrollment". ( <i>Id.</i> , at 23.)		
17b. receiving the biometric signal;	The Accused Instrumentalities are configured to receive the biometric signal.		
	More specifically, the iPhone has at least one biometric sensor for capturing a fingerprint or a face (Touch ID and/or Face ID), namely a Touch ID sensor and a camera system with image sensor, respectively.		
	Touch ID		
	"Apple devices with a Touch ID sensor can be unlocked using a fingerprint." (Ex. A, Apple Platform Security, at 19.)		
	"Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the <b>sensor</b> continuing to expand the fingerprint map as additional overlapping nodes are identified with each use."		

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 219 of 232

Claim 17	Accused Instrumentalities				
	<ul> <li>(<i>Id.</i>)</li> <li>"When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave."</li> <li>(<i>Id.</i>)</li> </ul>				
	The biometric sensor for Touch ID is located below the home button:				
	"The Home button is a stack of different materials, capped with a sapphire crystal lens. The surrounding stainless-steel ring works as a ground and detects the user's finger. This action activates a capacitive touch sensor installed underneath the cover: A CMOS chip with small capacitors." (https://appleinsider.com/inside/touch-id)				
	Biometric sensor 121				
	"Where is the Touch ID sensor located?				

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 220 of 232

<u>Claim 17</u>	Accused Instrumentalities
	The Touch ID sensor is located either in the home button or - on the iPad Air (4th generation) - in the top button.
	(https://support.apple.com/en-us/HT201371)
	The image sensor captures an 88-by-88-pixel, 500 PPI raster scan:
	"The 88-by-88-pixel, 500-ppi raster scan is temporarily stored in encrypted memory within the Secure Enclave while being vectorized for analysis, and then it's discarded. The analysis utilizes subdermal ridge flow angle mapping, which is a lossy process that discards minutia data that would be required to reconstruct the user's actual fingerprint. The resulting map of nodes is stored without any identity information in an encrypted format that can only be read by the Secure Enclave, and is never sent to Apple or backed up to iCloud or iTunes." (Ex. C, iOS Security white paper, at 8.)
	Face ID
	The biometric sensor for facial biometrics is a camera system ("TrueDepth camera system") with an image sensor.
	"With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face." (Ex. A, Apple Platform Security, at 20.)
	To receive a biometric signal, the camera system with image sensor reads over 30,000 infrared points to capture depth information along with a two-dimensional infrared image.
	"After the TrueDepth camera confirms the presence of an attentive face, it projects and <b>reads over</b> 30,000 infrared dots to form a depth map of the face along with a 2D infrared image. This data is

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 221 of 232

<u>Claim 17</u>	Accused Instrumentalities					
	Secure Enclave. To co sequence of 2D image portion of the Secure mathematical represen facial data is itself a m ( <i>Id.</i> , at 20.)	ounter both di es and depth r Neural Engin ntation and co nathematical cludes a bion	igital nap c e-pro ompa repre	and physica aptures, and tected within res that repre- sentation of	I spoofs, the Truel projects a device n the Secure Encla esentation to the en the user's face cap	digitally signed and sent to t Depth camera randomizes th specific random pattern. A we-transforms this data into nrolled facial data. This enro tured across a variety of pos
	receiver Monimal, Bharp CMOS mails bission (1.4561) BBM COS promotion matter Tong Hang Shin	Incs: 2004002 - 000224 2022 0021 0021 002 003 004 004 004 004 004 004 004	0	Ambient light sensor Mostile AMS	Eront Correct Marchall Renchall Cowell Onfilm Conformation service (MAR's Solvy) Unit performant Langien, Genaus Actionals Marconal, HTM	Construction of the second sec
	a Constant a		Act	live_alignment		film: Viewi Active alignment equipment.
				•		ASM Pacific
	(https://appleinsider.co report)	om/articles/1	7/09/	09/inner-wo	rkings-of-apples-f	ace-id-camera-detailed-in-

ASSA ABLOY Ex. 1021 - Page 220 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

<u>Claim 17</u>	Accused Instrumentalities
17c. matching the biometric signal against members of the database	The Accused Instrumentalities include a transmitter controller configured to emit a secure access signal conveying information dependent upon said accessibility attribute.
of biometric signatures to thereby output an accessibility attribute;	More specifically, the iPhone's System on Chip (SOC), i.e. the Secure Enclave with its Secure Enclave Processor (SEP) or a Secure Neural Engine contained therein, is a means (103) to check a match of the biometric signal with elements of the biometric signature database.
	"The Secure Enclave is a system on chip (SoC) that is included on all recent iPhone, devices" (Ex. A, Apple Platform Security, at 7.)
	"During <b>matching</b> , the Secure Enclave <b>compares</b> incoming data from the biometric sensor against the stored templates <b>to determine whether to unlock the device</b> or respond that a match is valid (for Apple Pay, in-app, and other uses of Touch ID and Face ID). " ( <i>Id.</i> , at 19.)
	The biometric signal received from the biometric sensor ("incoming data from the biometric sensor") is thus checked by the Secure Enclave and its SEP with the elements of the database of biometric signatures 105, i.e. the "stored templates", for the presence of a match.
	For Touch ID, the Secure Enclave match verification is performed as follows:
	"The Secure Enclave is responsible for processing fingerprint data from the Touch ID sensor, determining if there is a match against registered fingerprints, and then enabling access or purchases on behalf of the user" (Ex. C, iOS Security white paper, at 7.)
	"During enrollment, the resulting map of nodes is stored in an encrypted format that can be read only by the Secure Enclave as a template to compare against for future matches" (Ex. A, Apple Platform Security, at 19.)

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 223 of 232

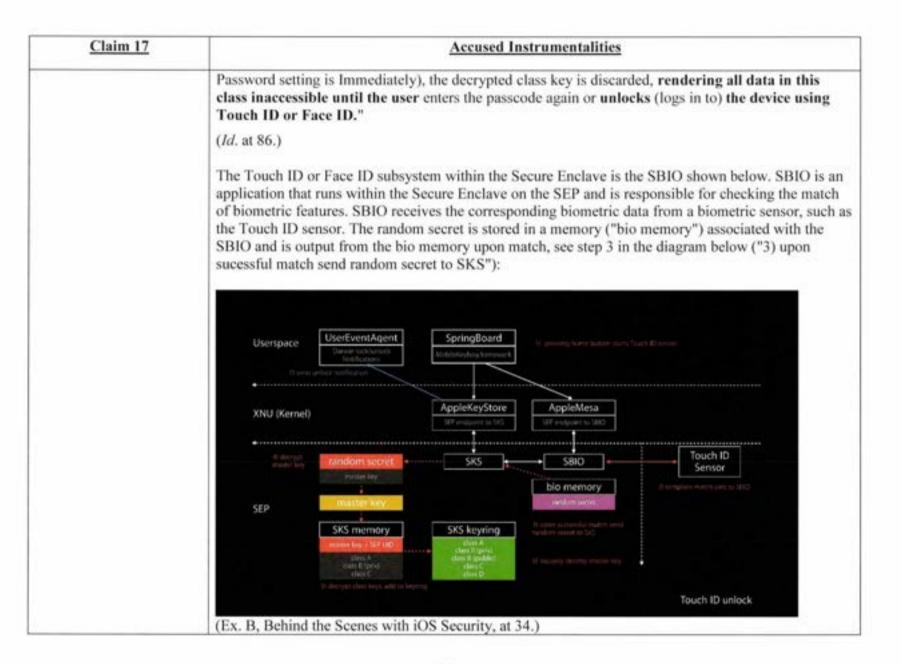
<u>Claim 17</u>	Accused Instrumentalities
	"Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. " (https://support.apple.com/en-us/HT204587)
	"Touch ID can read multiple fingerprints and recognize fingerprints at any orientation of the finger. The system then creates a mathematical representation of your fingerprint and compares it to the registered fingerprint data to determine a match and unlock your device." (https://support.apple.com/de-de/HT204587)
	For <b>Face ID</b> , the Secure Enclave has a neural network protected by it, i.e., a Secure Neural Engine, which is used to verify the match:
	"Face ID uses neural networks for determining attention, <b>matching</b> , and antispoofing, so a user can unlock their phone with a glance." (Ex. A, Apple Platform Security, at 20.)
	"A portion of the Secure Neural Engine-protected within the Secure Enclave-transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of the user's face captured across a variety of poses." ( <i>Id.</i> ).
	"Facial matching security
	Facial matching is performed within the Secure Enclave using neural networks trained specifically for that purpose Face ID data, including mathematical representations of a user's face, is encrypted and available only to the Secure Enclave. This data never leaves the device." ( <i>Id.</i> at 23.)
	When the Secure Enclave, or more precisely the Touch ID or Face ID subsystem within the Secure Enclave, has determined that a match exists, an accessibility attribute is issued by the corresponding

# Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 224 of 232

Claim 17	Accused Instrumentalities
	Touch ID or Face ID subsystem. This Touch ID or Face ID subsystem is also referred to as the SBIO. The accessibility attribute confirms that there is a match and that the iPhone is to be unlocked (" determine whether to unlock the device").
	This confirmation of the match is signaled by the SBIO by issuing a random secret to which only the Touch ID or Face ID subsystem within the Secure Enclave has access:
	"During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device []." ( <i>Id.</i> at 19.)
	"Uses for Touch ID and Face ID
	Unlocking a device or user account
	[] keys for the highest class of Data Protection-which are held in the Secure Enclave [].
	With Touch ID or Face ID enabled, the keys aren't discarded when the device or account locks; instead, <b>they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the</b> <b>Secure Enclave</b> . When a user attempts to unlock the device or account, <b>if the device detects a</b> <b>successful match, it provides the key for unwrapping the Data Protection keys</b> , and the device or account is unlocked. This process provides additional protection by requiring cooperation between the Data Protection and Touch ID or Face ID subsystems to unlock the device."
	( <i>Id.</i> at 24.)
	"The class key is protected with the hardware UID and, for some classes, the user's passcode." ( <i>Id.</i> at 85.)
	"Complete Protection
	(NSFileProtectionComplete): The class key is protected with a key derived from the user passcode or password and the device UID. Shortly after the user locks a device (10 seconds, if the Require

1

#### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 225 of 232

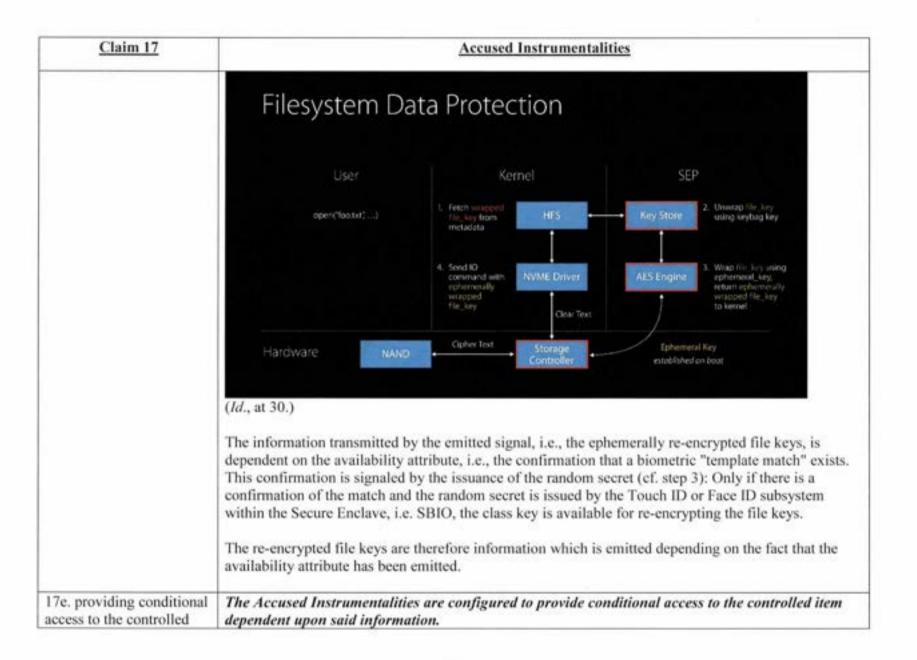


Claim 17	Accused Instrumentalities
	The class keys are encrypted with a master key:
	User Keybags
	Background
	Sets of keys generated for each user to protect their data at rest
	Keys wrapped by master key derived from user passcode and SEP UID
	After 10 incorrect passcode entries, SEP will not process any further attempts
	Different policy associated with each keybag key—Usage, availability
	( <i>Id.</i> , at 25.)
	The random secret is issued to SKS. SKS is a Secure Key Service application which is located within the Secure Enclave on the SEP and is responsible for decrypting class keys. The random secret provided by SBIO is used to decrypt a master key ("4) decrypt master key"). The master key is concatenated with the UID of the SEP and thus class keys are decrypted and added to the SKS keyring ("5) decrypt class keys, add to keyring") for further use by the Secure Enclave. The decrypted class keys include, for example, the class key of class A.
17d. emitting a secure access signal conveying information dependent upon said accessibility attribute; and	The Accused Instrumentalities include a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.         For example, the Secure Enclave emits a signal with ephemerally re-encrypted file keys:

## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 227 of 232

<u>Claim 17</u>	Accused Instrumentalities
	<ul> <li>"sepOS can then use the ephemeral wrapping key to wrap file keys for use by the Application</li> <li>Processor file-system driver. When the file-system driver reads or writes a file, it sends the wrapped key to the AES Engine."</li> <li>(Ex. A, Apple Platform Security, at 14.)</li> </ul>
	"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. [] When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." ( <i>Id.</i> at 85.)
	The signal with the ephemerally re-encrypted file keys is a secure signal because it comes from the Secure Enclave and thus from a secure environment. Furthermore, the signal is secure because the transmitted information is encrypted. The emitted file keys are encrypted with the ephemeral key:
	"All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the Application Processor. At startup, the Secure Enclave negotiates an ephemeral key with the AES Engine. When the Secure Enclave unwraps a file's keys, they're rewrapped with the ephemeral key and sent back to the Application Processor." ( <i>Id.</i> )

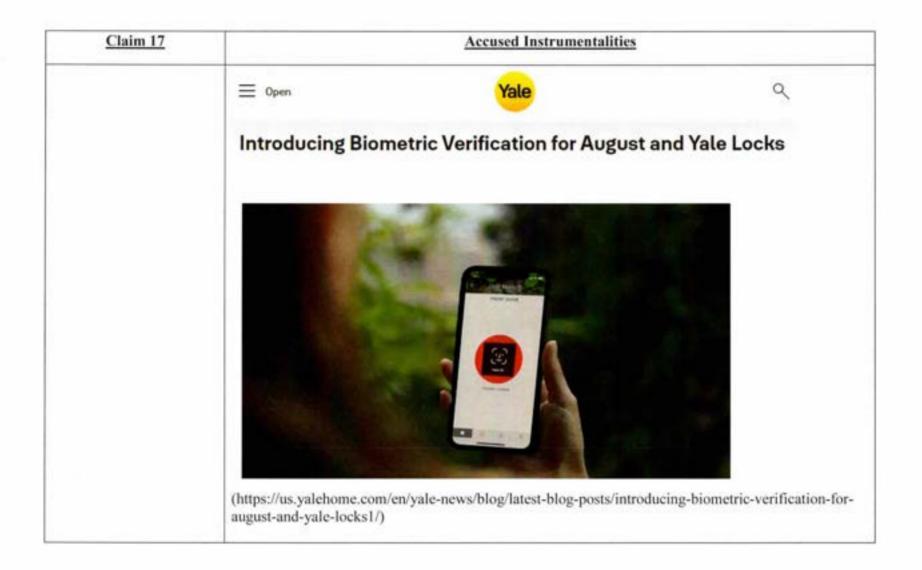
Claim 17	Accused Instrumentalities
	Filesystem Data Protection
	Overview
	File blocks are encrypted using AES-XTS with 128-bit keys
	Each file on the user partition is encrypted using a unique random key chosen by S
	Raw file keys are never exposed to the AP
	<ul> <li>Wrapped with a key from the user keybag for long-term storage</li> </ul>
	<ul> <li>Wrapped with an ephemeral key while in use, bound to boot session (Ex. B, Behind the Scenes with iOS Security, at 29.)</li> </ul>



## Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 230 of 232

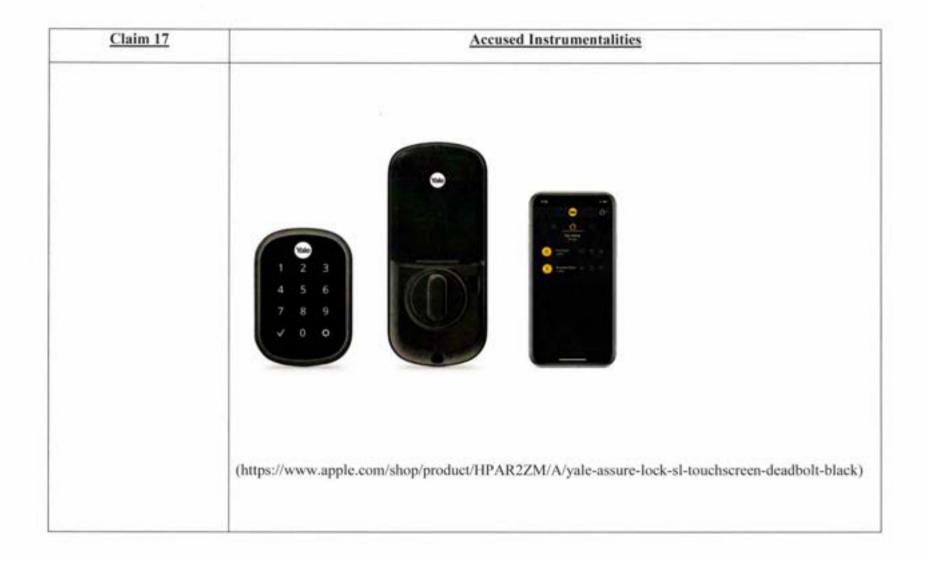
Claim 17	Accused Instrumentalities		
item dependent upon said information, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.	More specifically, the controlled item is a locking mechanism of the door lock of the user's home. The Accused Instrumentalities are configured to provide secure access to the user's home via Yale Smart Locks when the user provides biometric signal to the Accused Instrumentalities via Touch ID or Face ID. "When the "Secure Remote Access" feature is turned on, the app will use your phone's built-in authentication tools to prompt fingerprint or facial recognition before you can unlock or lock your home remotely (note: if your phone does not have these features, it will prompt you to use your PIN code). This further ensures that your door is only operated by the right people at the time you intend for it." (https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-		

### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 231 of 232



ASSA ABLOY Ex. 1021 - Page 230 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208

### Case 3:22-cv-00694 Document 1-9 Filed 05/23/22 Page 232 of 232



ASSA ABLOY Ex. 1021 - Page 231 ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd. IPR2022-01089 - U.S. Patent No. 9,269,208