IN THE UNITED STATES DISTRICT COURT
FOR DISTRICT OF DELAWARE

BIOMETRIC TECHNOLOGY HOLDINGS LLC,	)
	)
Plaintiff,	)
	) Civil Action No. ________________
v.	)
	) **JURY TRIAL DEMANDED**
SYNAPTICS INCORPORATED,	)
	)
Defendant.	)
____	)

COMPLAINT

For its Complaint, Biometric Technology Holdings LLC ("BTH"), by and through the undersigned counsel, alleges as follows:

THE PARTIES

1. BTH is a Delaware limited liability company with a place of business located at 3511 Silverside Road, Suite 105, Wilmington, Delaware 19810.

2. Defendant Synaptics Incorporated is a Delaware company with, upon information and belief, a place of business located at 1440 Main Street, Waltham, Massachusetts 02451.

JURISDICTION AND VENUE

3. This action arises under the Patent Act, 35 U.S.C. § 1 *et seq.*

4. Subject matter jurisdiction is proper in this Court under 28 U.S.C. §§ 1331 and 1338.

5. Upon information and belief, Defendant conducts substantial business in this forum, directly or through intermediaries, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct and/or deriving substantial revenue from goods and services provided to individuals in this district.

6. Venue is proper in this district pursuant to § 1400(b).

THE PATENT-IN-SUIT

7. On April 17, 2001, U.S. Patent No. 6,219,439 (the "'439 patent"), entitled "Biometric Authentication System," was duly and lawfully issued by the U.S. Patent and Trademark Office. A true and correct copy of the '439 patent is attached hereto as Exhibit A.

8. BTH is the assignee and owner of the right, title and interest in and to the '439 patent, including the right to assert all causes of action arising under said patent and the right to any remedies for infringement of it.

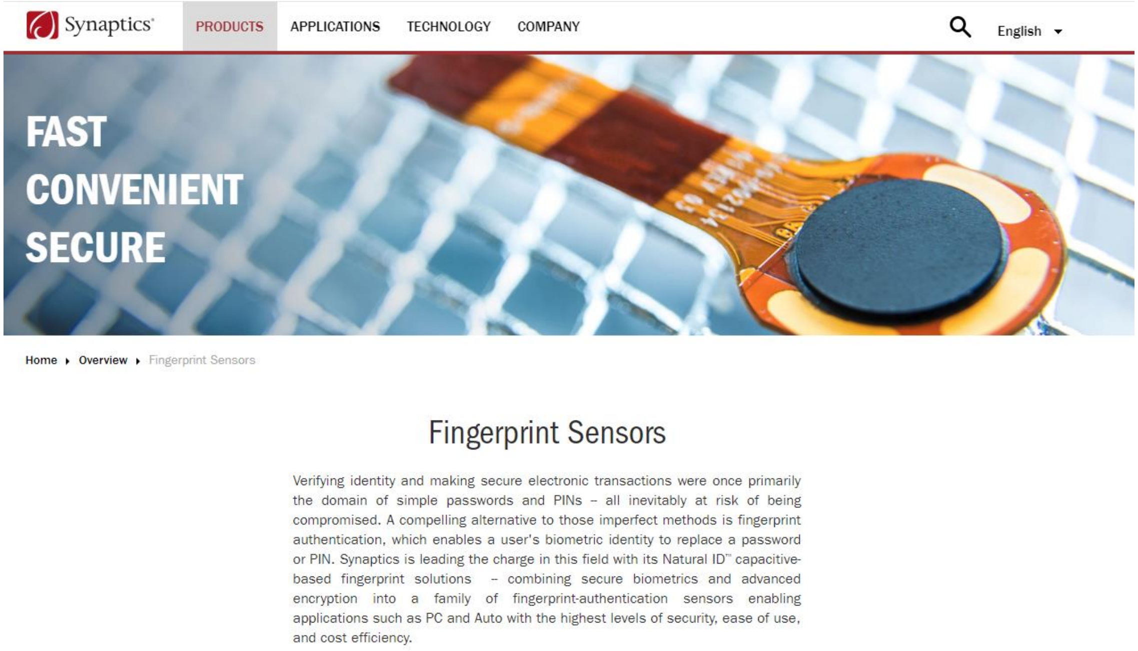
COUNT I – INFRINGEMENT OF U.S. PATENT NO. 6,219,439

9. BTH repeats and realleges the allegations of paragraphs 1 through 8 as if fully set forth herein.

10. Without license or authorization and in violation of 35 U.S.C. § 271(a), Defendant has infringed and continues to infringe at least claim 4 of the '439 patent by making, using, importing, offering for sale, and/or selling, methods and apparatuses for authenticating a user, including, but not limited to, Synaptics Natural ID Fingerprint Sensors with SentryPoint Security Suite (the "Accused Device"), because each and every element is met either literally or equivalently.

11. Upon information and belief, Defendant used the Accused Device via its internal use and testing in the United States, directly infringing one or more claims of the '439 patent.

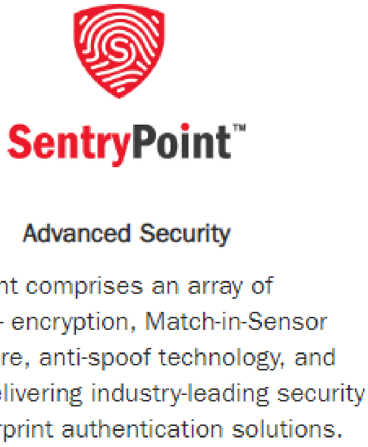
12. More specifically, the Accused Device is an authentication apparatus.



Fingerprint Sensors

Verifying identity and making secure electronic transactions were once primarily the domain of simple passwords and PINs – all inevitably at risk of being compromised. A compelling alternative to those imperfect methods is fingerprint authentication, which enables a user's biometric identity to replace a password or PIN. Synaptics is leading the charge in this field with its Natural ID™ capacitive-based fingerprint solutions – combining secure biometrics and advanced encryption into a family of fingerprint-authentication sensors enabling applications such as PC and Auto with the highest levels of security, ease of use, and cost efficiency.

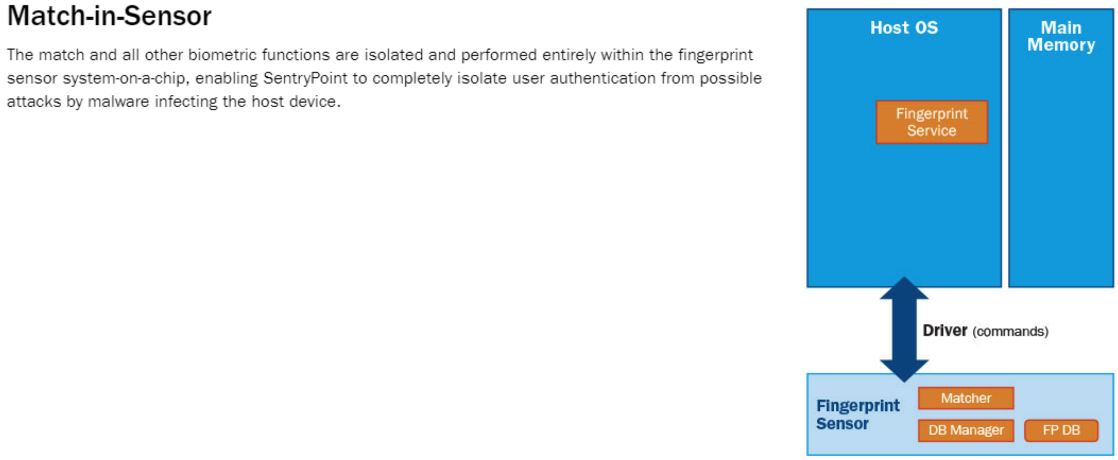
https://www.synaptics.com/products/biometrics.



Advanced Security

SentryPoint comprises an array of features – encryption, Match-in-Sensor architecture, anti-spoof technology, and more – delivering industry-leading security and fingerprint authentication solutions.

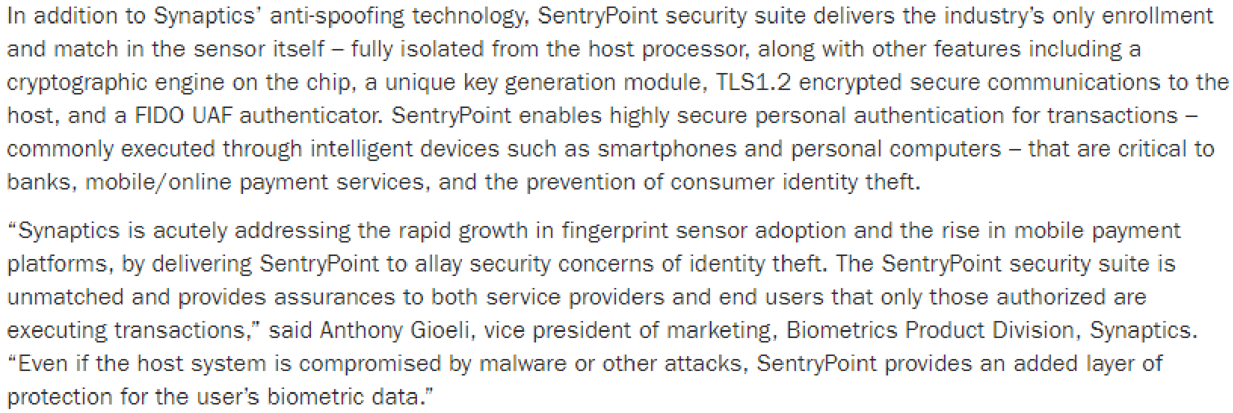
Id.



Match-in-Sensor

The match and all other biometric functions are isolated and performed entirely within the fingerprint sensor system-on-a-chip, enabling SentryPoint to completely isolate user authentication from possible attacks by malware infecting the host device.

https://www.synaptics.com/technology/security-suite.

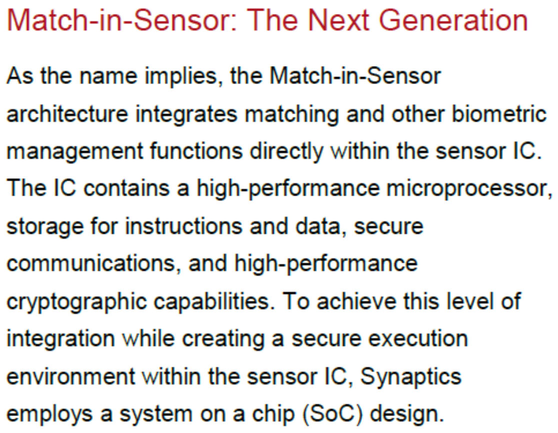


In addition to Synaptics' anti-spoofing technology, SentryPoint security suite delivers the industry's only enrollment and match in the sensor itself – fully isolated from the host processor, along with other features including a cryptographic engine on the chip, a unique key generation module, TLS1.2 encrypted secure communications to the host, and a FIDO UAF authenticator. SentryPoint enables highly secure personal authentication for transactions – commonly executed through intelligent devices such as smartphones and personal computers – that are critical to banks, mobile/online payment services, and the prevention of consumer identity theft.

"Synaptics is acutely addressing the rapid growth in fingerprint sensor adoption and the rise in mobile payment platforms, by delivering SentryPoint to allay security concerns of identity theft. The SentryPoint security suite is unmatched and provides assurances to both service providers and end users that only those authorized are executing transactions," said Anthony Gioeli, vice president of marketing, Biometrics Product Division, Synaptics. "Even if the host system is compromised by malware or other attacks, SentryPoint provides an added layer of protection for the user's biometric data."

https://www.synaptics.com/company/news/sentrypoint-anti-spoofing.

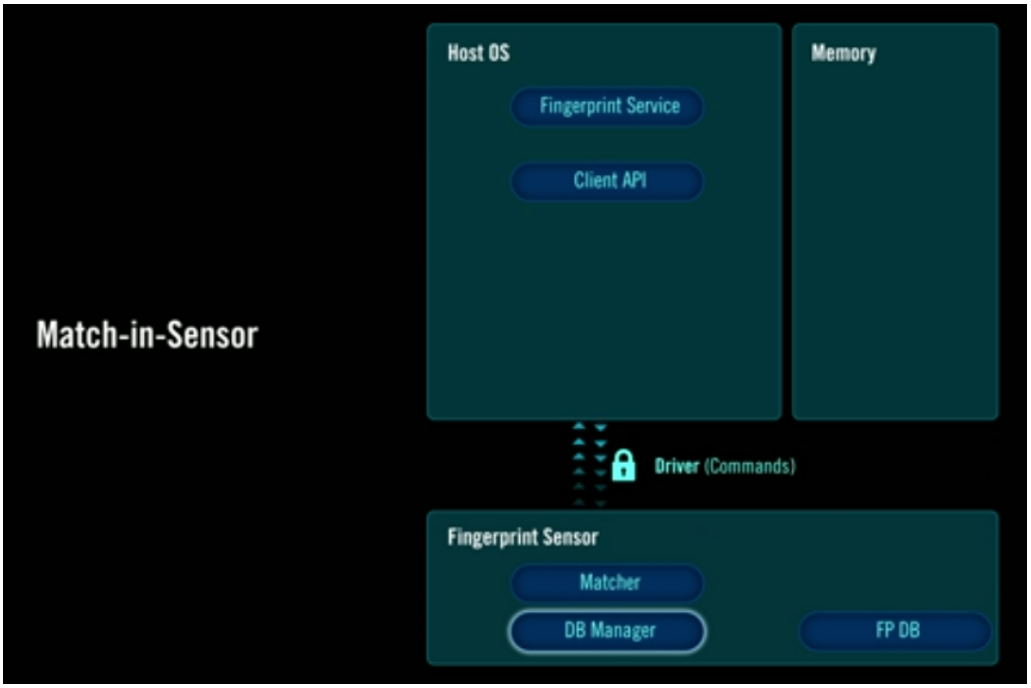
13. The Accused Device includes a storage means for storing biometric data of a user.



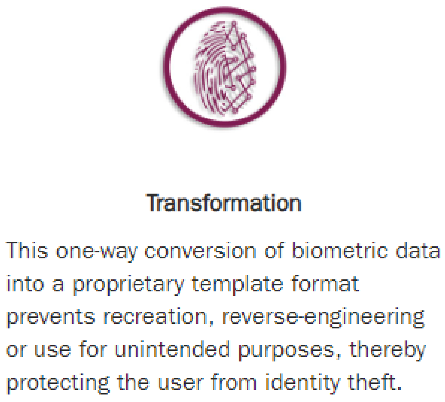
Match-in-Sensor: The Next Generation

As the name implies, the Match-in-Sensor architecture integrates matching and other biometric management functions directly within the sensor IC. The IC contains a high-performance microprocessor, storage for instructions and data, secure communications, and high-performance cryptographic capabilities. To achieve this level of integration while creating a secure execution environment within the sensor IC, Synaptics employs a system on a chip (SoC) design.

Fingerprint Sensing: The Next Generation ("Fingerprint Sensing") at p. 3 (available at https://www.synaptics.com/sites/default/files/fingerprint-sensing-biometric-security.pdf).



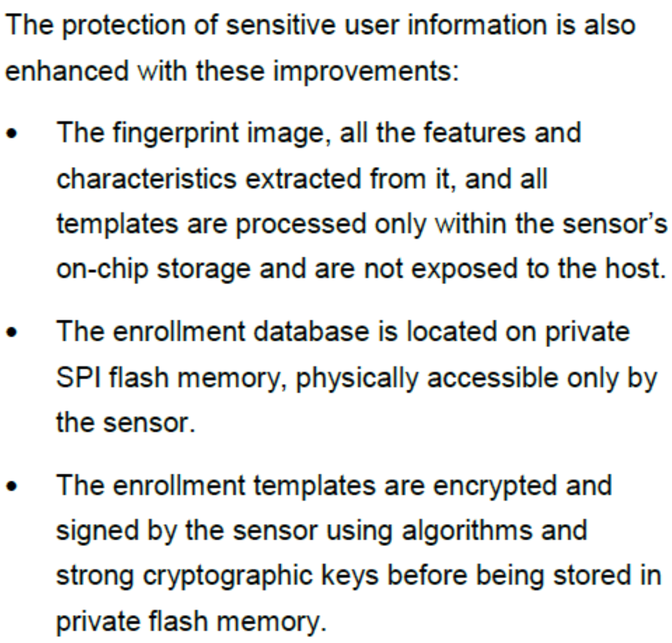
http://players.brightcove.net/4709052657001/default_default/index.html?videoId=4710089007001.



Transformation

This one-way conversion of biometric data into a proprietary template format prevents recreation, reverse-engineering or use for unintended purposes, thereby protecting the user from identity theft.

https://www.synaptics.com/technology/security-suite.

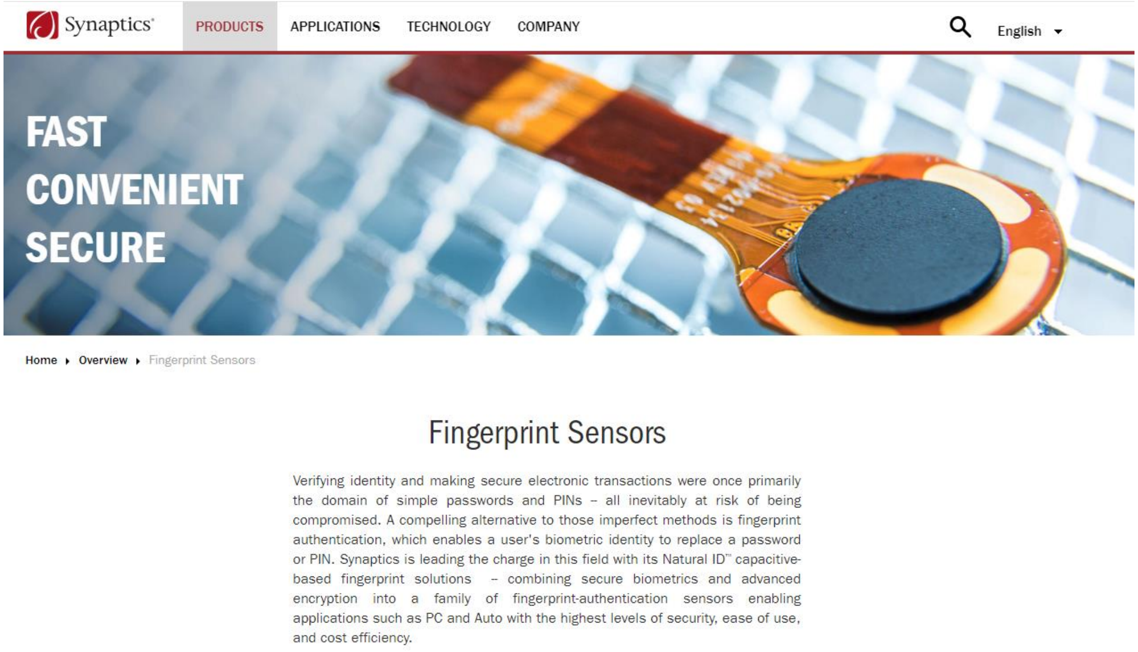


The protection of sensitive user information is also enhanced with these improvements:

- The fingerprint image, all the features and characteristics extracted from it, and all templates are processed only within the sensor's on-chip storage and are not exposed to the host.
- The enrollment database is located on private SPI flash memory, physically accessible only by the sensor.
- The enrollment templates are encrypted and signed by the sensor using algorithms and strong cryptographic keys before being stored in private flash memory.

Fingerprint Sensing at p. 3.

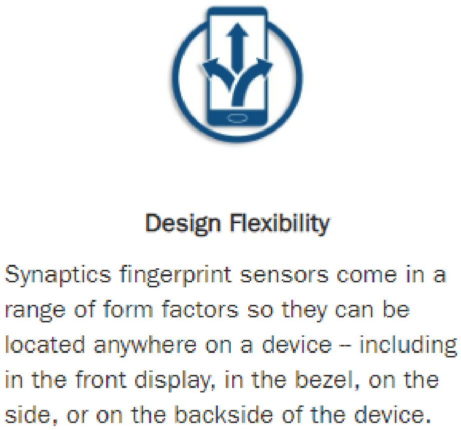
14. The Accused Device includes reader means for reading a biometric feature of a user.



Fingerprint Sensors

Verifying identity and making secure electronic transactions were once primarily the domain of simple passwords and PINs – all inevitably at risk of being compromised. A compelling alternative to those imperfect methods is fingerprint authentication, which enables a user's biometric identity to replace a password or PIN. Synaptics is leading the charge in this field with its Natural ID™ capacitive-based fingerprint solutions – combining secure biometrics and advanced encryption into a family of fingerprint-authentication sensors enabling applications such as PC and Auto with the highest levels of security, ease of use, and cost efficiency.

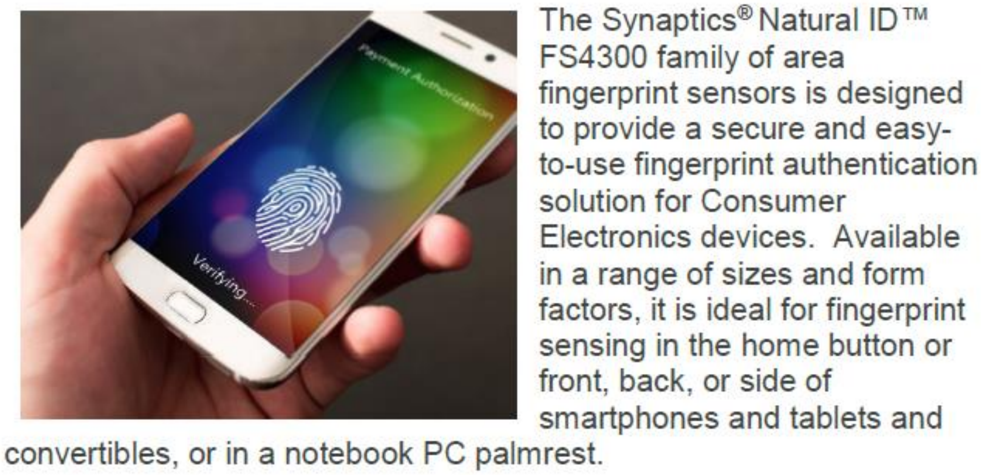
https://www.synaptics.com/products/biometrics.



Design Flexibility

Synaptics fingerprint sensors come in a range of form factors so they can be located anywhere on a device – including in the front display, in the bezel, on the side, or on the backside of the device.

https://www.synaptics.com/products/biometrics.

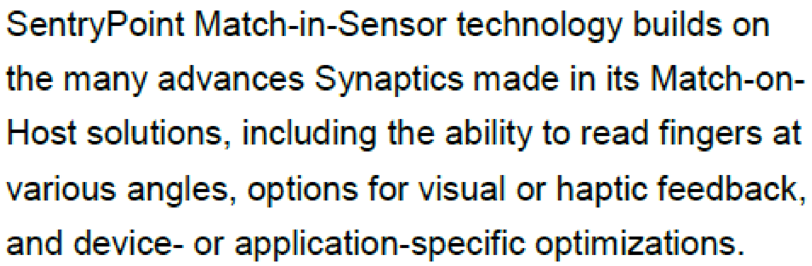


Payment Authorization
Verifying...

The Synaptics® Natural ID™ FS4300 family of area fingerprint sensors is designed to provide a secure and easy-to-use fingerprint authentication solution for Consumer Electronics devices. Available in a range of sizes and form factors, it is ideal for fingerprint sensing in the home button or front, back, or side of smartphones and tablets and convertibles, or in a notebook PC palmrest.

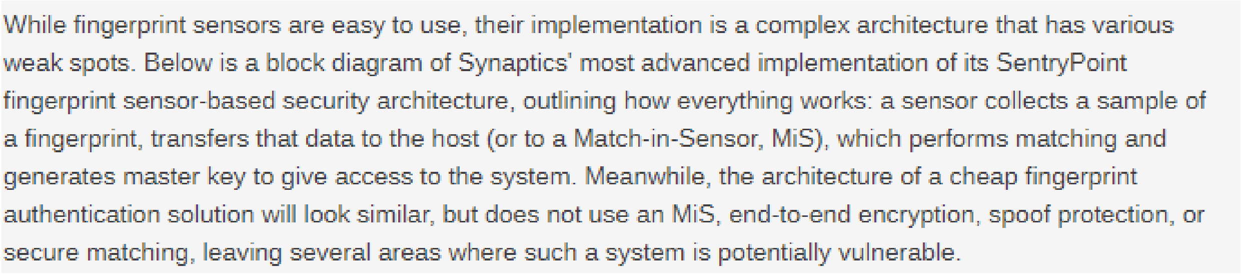
FS4300 Family Touch Fingerprint Sensor Product Brief at p. 1 (available at https://www.synaptics.com/sites/default/files/fs4300-product-brief.pdf).

https://www.synaptics.com/sites/default/files/Bio_Natural-ID_1_Sm_0.jpg.



SentryPoint Match-in-Sensor technology builds on the many advances Synaptics made in its Match-on-Host solutions, including the ability to read fingers at various angles, options for visual or haptic feedback, and device- or application-specific optimizations.

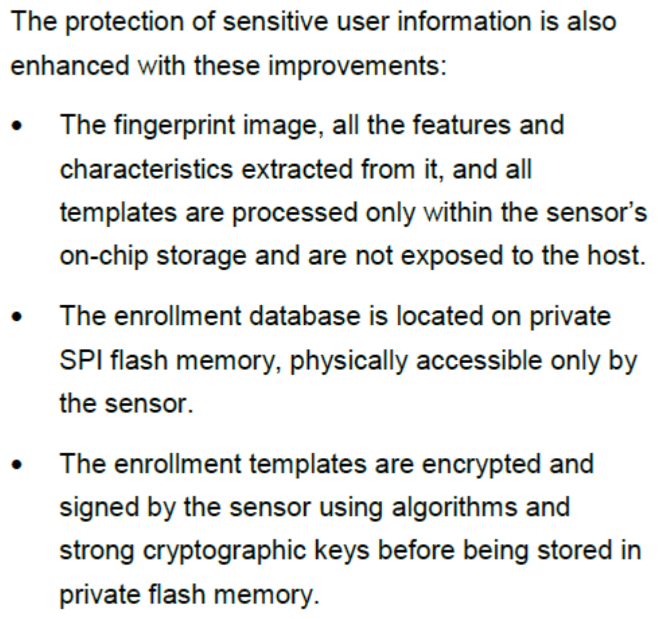
Fingerprint Sensing at p. 4.



While fingerprint sensors are easy to use, their implementation is a complex architecture that has various weak spots. Below is a block diagram of Synaptics' most advanced implementation of its SentryPoint fingerprint sensor-based security architecture, outlining how everything works: a sensor collects a sample of a fingerprint, transfers that data to the host (or to a Match-in-Sensor, MiS), which performs matching and generates master key to give access to the system. Meanwhile, the architecture of a cheap fingerprint authentication solution will look similar, but does not use an MiS, end-to-end encryption, spoof protection, or secure matching, leaving several areas where such a system is potentially vulnerable.

https://www.anandtech.com/show/11444/synaptics-discusses-fingerprint-encryption.

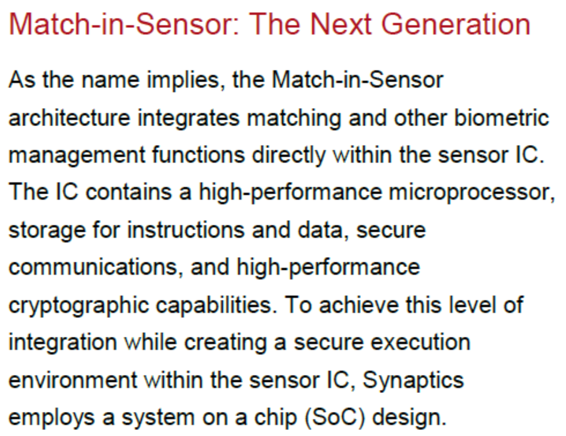
15. The reader means coacts with the storage means for reading the biometric data at the reader means.



The protection of sensitive user information is also enhanced with these improvements:

- The fingerprint image, all the features and characteristics extracted from it, and all templates are processed only within the sensor's on-chip storage and are not exposed to the host.
- The enrollment database is located on private SPI flash memory, physically accessible only by the sensor.
- The enrollment templates are encrypted and signed by the sensor using algorithms and strong cryptographic keys before being stored in private flash memory.

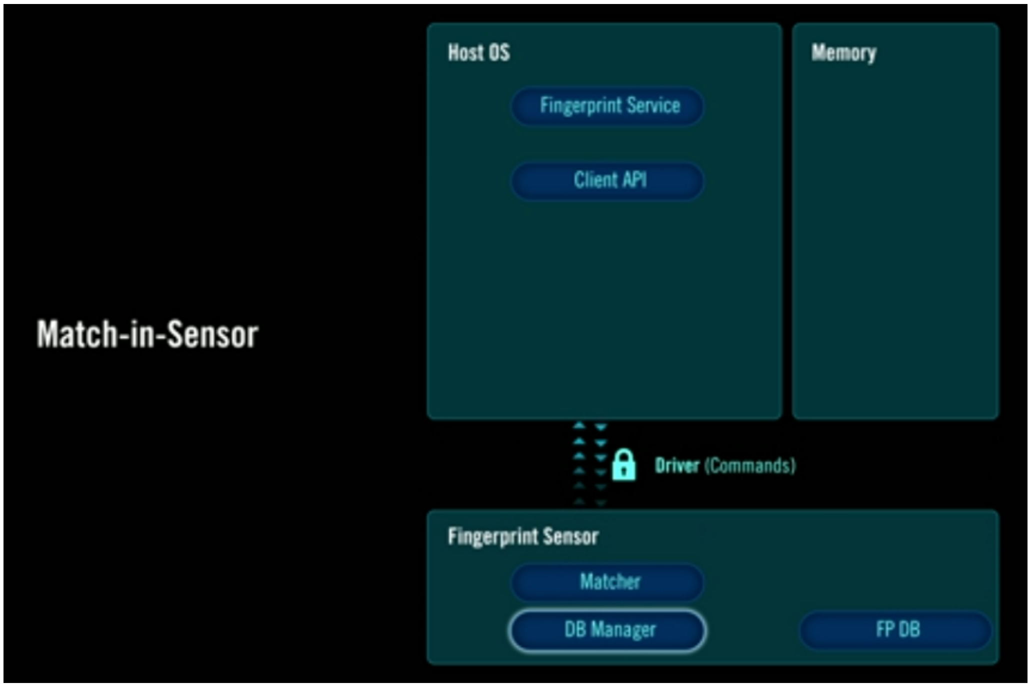
Fingerprint Sensing at p. 3.



Match-in-Sensor: The Next Generation

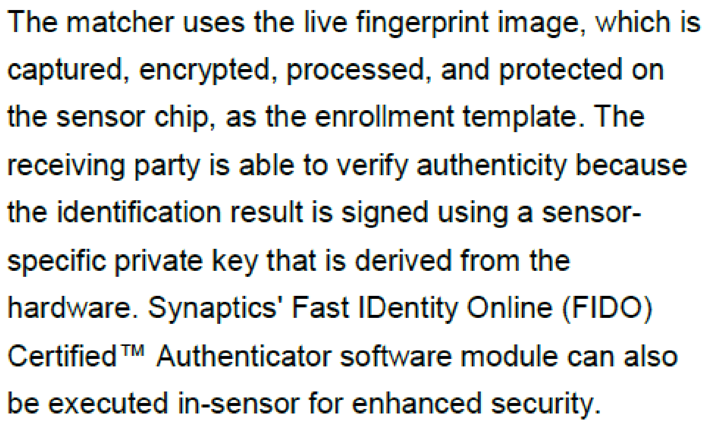
As the name implies, the Match-in-Sensor architecture integrates matching and other biometric management functions directly within the sensor IC. The IC contains a high-performance microprocessor, storage for instructions and data, secure communications, and high-performance cryptographic capabilities. To achieve this level of integration while creating a secure execution environment within the sensor IC, Synaptics employs a system on a chip (SoC) design.

Fingerprint Sensing at p. 3.



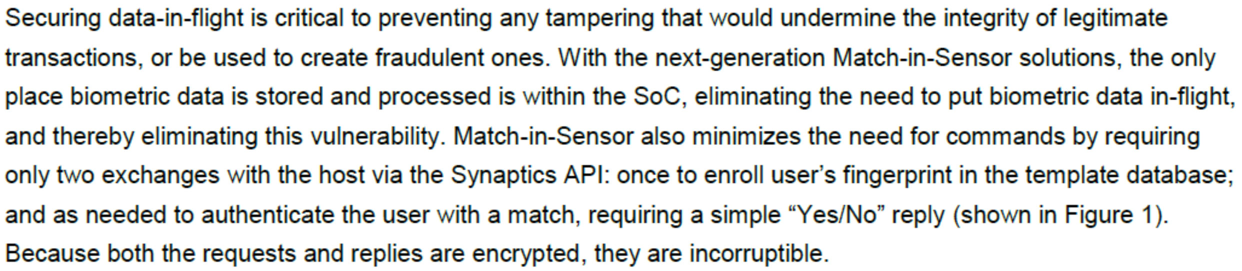
http://players.brightcove.net/4709052657001/default_default/index.html?videoId=4710089007001.

16. The reader means generates a signal representing a result of a comparison of the biometric data with the biometric feature of the user to determine authentication status of the user.



The matcher uses the live fingerprint image, which is captured, encrypted, processed, and protected on the sensor chip, as the enrollment template. The receiving party is able to verify authenticity because the identification result is signed using a sensor-specific private key that is derived from the hardware. Synaptics' Fast IDentity Online (FIDO) Certified™ Authenticator software module can also be executed in-sensor for enhanced security.

Fingerprint Sensing at p. 3.



Securing data-in-flight is critical to preventing any tampering that would undermine the integrity of legitimate transactions, or be used to create fraudulent ones. With the next-generation Match-in-Sensor solutions, the only place biometric data is stored and processed is within the SoC, eliminating the need to put biometric data in-flight, and thereby eliminating this vulnerability. Match-in-Sensor also minimizes the need for commands by requiring only two exchanges with the host via the Synaptics API: once to enroll user's fingerprint in the template database; and as needed to authenticate the user with a match, requiring a simple "Yes/No" reply (shown in Figure 1). Because both the requests and replies are encrypted, they are incorruptible.

SentryPoint Encryption ("SentryPoint Encryption") at p. 4 (available at https://www.synaptics.com/sites/default/files/sentrypoint-encryption.pdf).

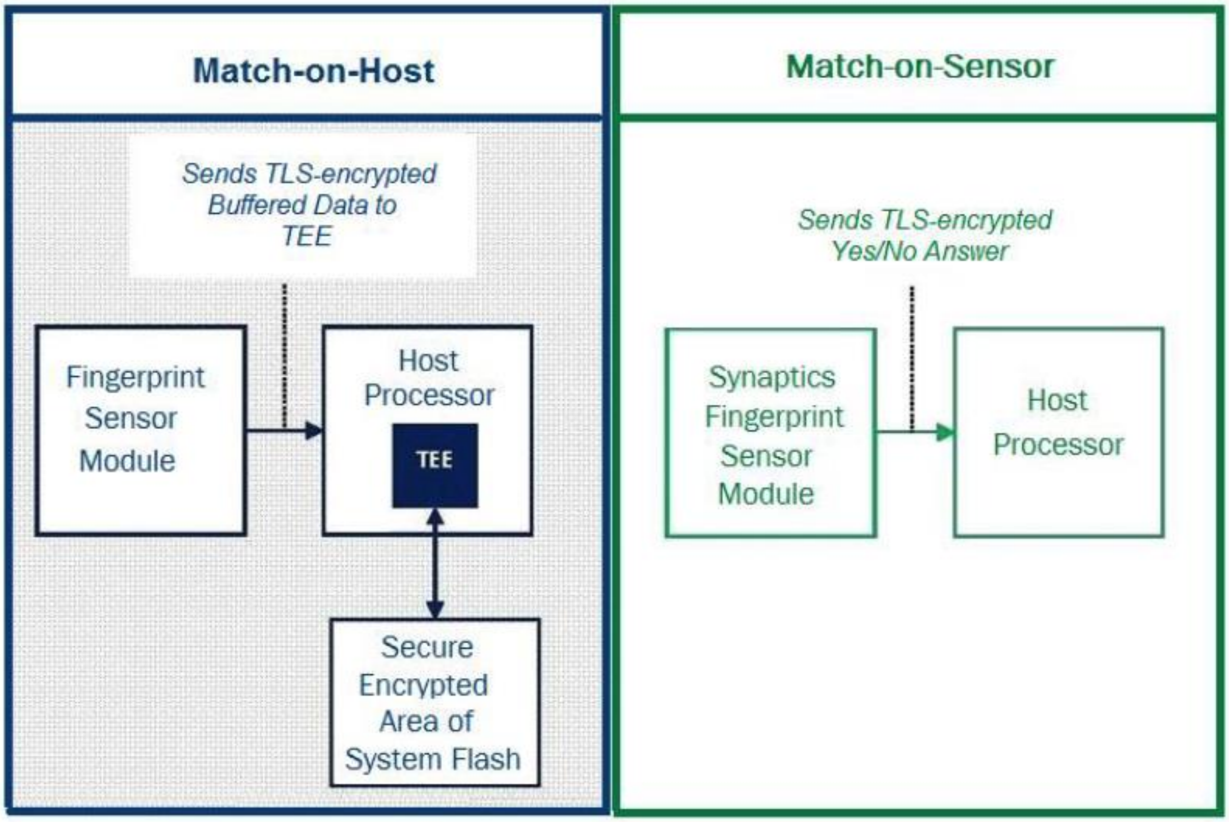
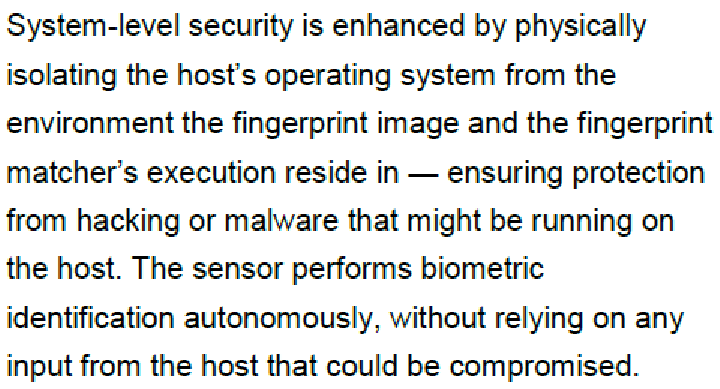

Match-on-Host
Sends TLS-encrypted Buffered Data to TEE
Fingerprint Sensor Module
Host Processor
TEE
Secure Encrypted Area of System Flash
Match-on-Sensor
Sends TLS-encrypted Yes/No Answer
Synaptics Fingerprint Sensor Module
Host Processor

Figure 1. Match-on-Host and Match-in-Sensor

Id.

17. The Accused Device includes control means in communication with the reader means for controlling access to the biometric data and the biometric feature of the user to be restricted to the reader means until positive authentication of the user.



System-level security is enhanced by physically isolating the host's operating system from the environment the fingerprint image and the fingerprint matcher's execution reside in — ensuring protection from hacking or malware that might be running on the host. The sensor performs biometric identification autonomously, without relying on any input from the host that could be compromised.

Fingerprint Sensing at p. 3.

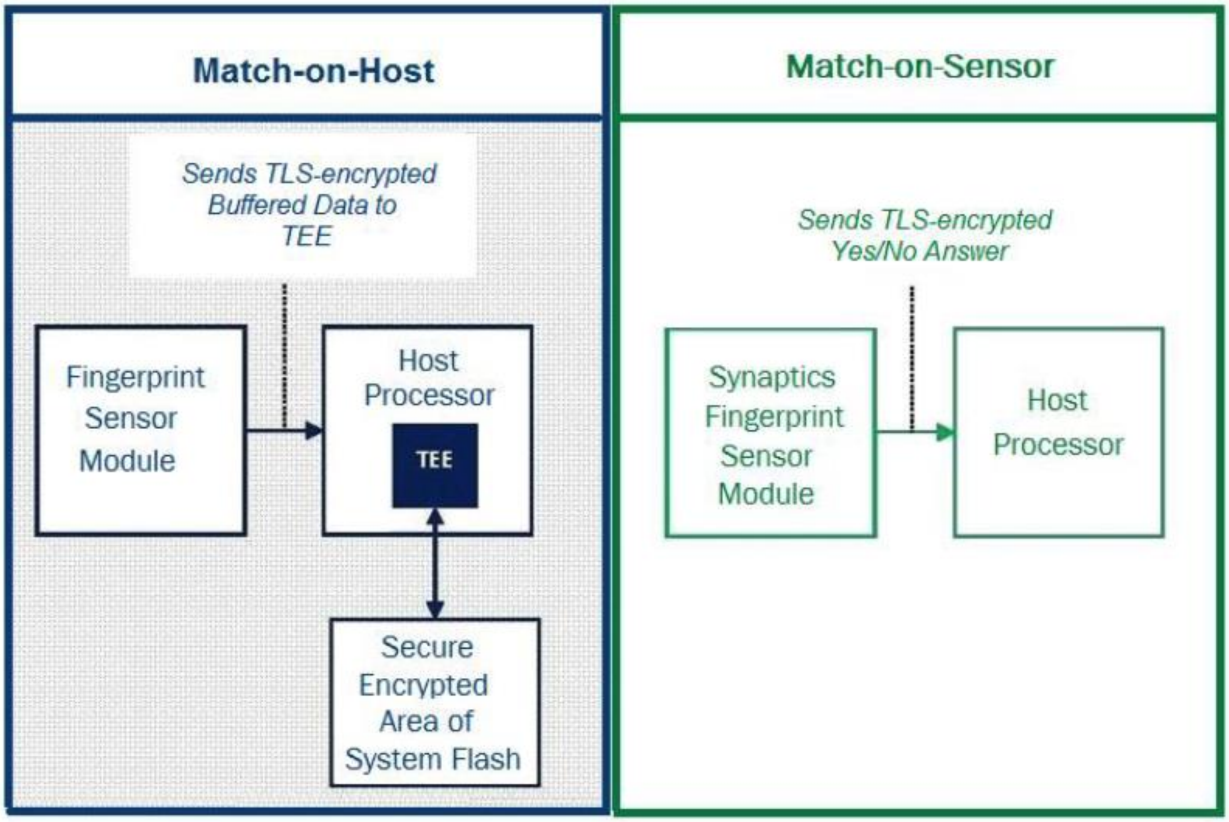
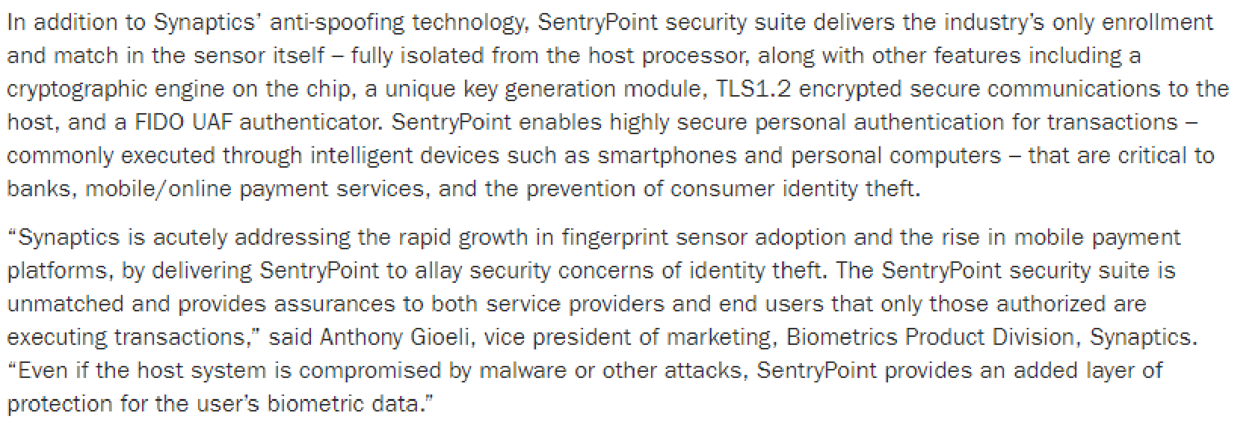

Match-on-Host
Sends TLS-encrypted Buffered Data to TEE
Fingerprint Sensor Module
Host Processor
TEE
Secure Encrypted Area of System Flash
Match-on-Sensor
Sends TLS-encrypted Yes/No Answer
Synaptics Fingerprint Sensor Module
Host Processor

Figure 1. Match-on-Host and Match-in-Sensor

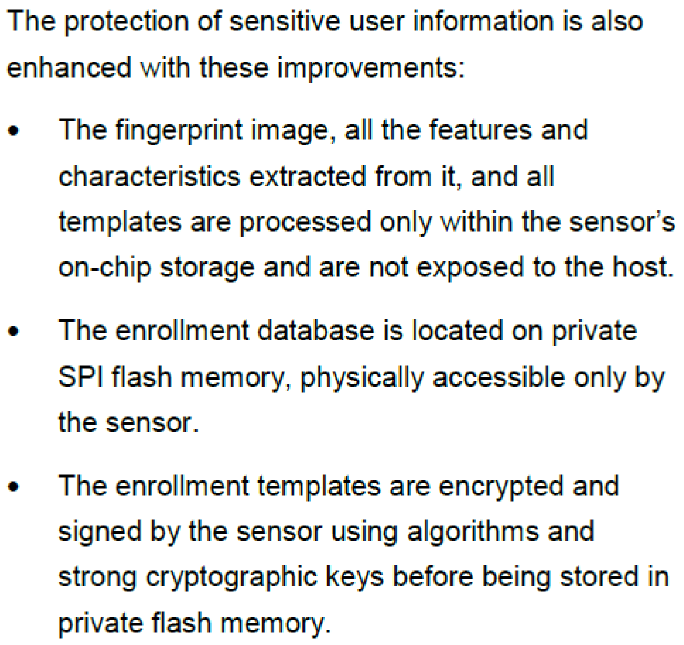
SentryPoint Encryption at p. 4.



In addition to Synaptics' anti-spoofing technology, SentryPoint security suite delivers the industry's only enrollment and match in the sensor itself – fully isolated from the host processor, along with other features including a cryptographic engine on the chip, a unique key generation module, TLS1.2 encrypted secure communications to the host, and a FIDO UAF authenticator. SentryPoint enables highly secure personal authentication for transactions – commonly executed through intelligent devices such as smartphones and personal computers – that are critical to banks, mobile/online payment services, and the prevention of consumer identity theft.

"Synaptics is acutely addressing the rapid growth in fingerprint sensor adoption and the rise in mobile payment platforms, by delivering SentryPoint to allay security concerns of identity theft. The SentryPoint security suite is unmatched and provides assurances to both service providers and end users that only those authorized are executing transactions," said Anthony Gioeli, vice president of marketing, Biometrics Product Division, Synaptics. "Even if the host system is compromised by malware or other attacks, SentryPoint provides an added layer of protection for the user's biometric data."

https://www.synaptics.com/company/news/sentrypoint-anti-spoofing.



The protection of sensitive user information is also enhanced with these improvements:

- The fingerprint image, all the features and characteristics extracted from it, and all templates are processed only within the sensor's on-chip storage and are not exposed to the host.
- The enrollment database is located on private SPI flash memory, physically accessible only by the sensor.
- The enrollment templates are encrypted and signed by the sensor using algorithms and strong cryptographic keys before being stored in private flash memory.

Fingerprint Sensing at p. 3.

18. BTH is entitled to recover from Defendant the damages sustained by BTH as a result of Defendant's infringement of the '439 patent in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

JURY DEMAND

BTH hereby demands a trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, BTH requests that this Court enter judgment against Defendant as follows:

A. An adjudication that Defendant has infringed the '439 patent;

B. An award of damages to be paid by Defendant adequate to compensate BTH for Defendant's past infringement of the '439 patent and any continuing or future infringement through the date such judgment is entered, including interest, costs, expenses and an accounting of all infringing acts including, but not limited to, those acts not presented at trial;

C. A declaration that this case is exceptional under 35 U.S.C. § 285, and an award of BTH's reasonable attorneys' fees; and

D. An award to BTH of such further relief at law or in equity as the Court deems just and proper.

Dated: July 2, 2019

STAMOULIS & WEINBLATT LLC

/s/ Richard C. Weinblatt
Stamatios Stamoulis (#4606)
Richard C. Weinblatt (#5080)
800 N. West Street, Third Floor
Wilmington, DE 19801
(302) 999-1540
stamoulis@swdelaw.com
weinblatt@swdelaw.com

Attorneys for Plaintiff
Biometric Technology Holdings LLC