UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

CONFIRMETRICS, LLC, Plaintiff v. **THREATMARK, INC.,** Defendant	**CIVIL ACTION NO. 6:22-cv-487** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Confirmetrics, LLC files this Complaint against Defendant ThreatMark, Inc. for infringement of three United States patents: U.S. Patent Nos. 8,838,967, 9,603,016, and 9,801,048.

THE PARTIES

1. Plaintiff and patent owner Confirmetrics is a Texas limited liability company with its headquarters and principal place of business in Plano, Texas.

2. Defendant ThreatMark is a Delaware corporation with a principal place of business at 1570 Legacy Town Center, 6860 Dallas Parkway, Suite 200, Plano, Texas 75024.

3. On information and belief, ThreatMark is affiliated with a company by the same name founded in the Czech Republic in 2015.

4. ThreatMark may be served through its registered agent The Corporation Trust Company, at Corporation Trust Center 1209 Orange St., Wilmington, Delaware, 19801.

JURISDICTION AND VENUE

5. This is a patent suit brought under the United States Patent Act, namely 35 U.S.C. §§ 271, 281, and 284-285, among other laws.

6. This Court has subject-matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

7. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391 and 28 U.S.C. § 1400(b). ThreatMark markets, sells, offers to sell, and delivers accused products in this district, directs and instructs customers and end users how to use the accused products in this district, and has committed acts of infringement in this district.

8. ThreatMark maintains an established place of business at 1570 Legacy Town Center, 6860 Dallas Parkway St. #200, Plano, Texas, 75024. This Court has personal jurisdiction over ThreatMark by virtue of its transaction of business and acts of patent infringement that have been committed in the State of Texas and in this judicial district.

THE ASSERTED PATENTS

9. Confirmetrics is the owner by assignment of all rights, title, and

interest in and to United States Patent Number 8,838,967 (the "'967 Patent"), titled UNIQUELY IDENTIFYING A MOBILE ELECTRONIC DEVICE, including the right to sue for all past, present, and future infringement. Exhibit A is a true and correct copy of the '967 Patent.

10. After a full and fair examination, the Patent Office issued the '967 Patent on September 16, 2014. The '967 Patent claims priority to application No. 61/324,312 (the "Provisional Application") filed on April 15, 2010.

11. The '967 Patent is valid and enforceable.

12. Confirmetrics is the owner by assignment of all rights, title, and interest in and to United States Patent Number 9,603,016 (the "'016 Patent"), titled UNIQUELY IDENTIFYING A MOBILE ELECTRONIC DEVICE, including the right to sue for all past, present, and future infringement. Exhibit B is a true and correct copy of the '016 Patent.

13. After a full and fair examination, the Patent Office issued the '016 Patent on March 21, 2017. The '016 Patent is a continuation of the application that issued as the '967 Patent and claims priority to the Provisional Application filed on April 15, 2010.

14. The '016 Patent is valid and enforceable.

15. Confirmetrics is the owner by assignment of all rights, title, and interest in and to United States Patent Number 9,801,048 (the "'048 Patent"), titled

UNIQUELY IDENTIFYING A MOBILE ELECTRONIC DEVICE. including the right to sue for all past, present, and future infringement. Exhibit C is a true and correct copy of the '048 Patent.

16. After a full and fair examination, the Patent office issued the '048 Patent on October 24, 2017. The '048 Patent is a continuation of the application that issued as the '016 Patent and claims priority to the Provisional Application filed on April 15, 2010.

17. The '048 Patent is valid and enforceable.

18. The Asserted Patents relate to "method[s] of watermarking mobile devices using their configuration settings so that remote systems trust interacting with them more." '967 Patent at col. 1:23-25.

19. The inventors of the Asserted Patents recognized that "[M]obile devices typically contain tons of configuration settings, and mobile phones in particular have contact lists (which represent a lot of information), so each mobile device will be found to be very different from every other." *Id.* at col. 3:1-4.

20. The inventors of the Asserted Patents recognized that "the advantage of our invention is that it uses a mobile device's configuration settings to uniquely identify it." *Id.* at col. 2:66-3:1.

21. Before Confirmetrics' inventions, "[e]xisting methods of identifying a mobile device" were limited and included use of an International Mobile

Equipment Identity (IMEI) number, where an IMEI number is given to every phone using most of the newest cell networks. However, accessing the IMEI number of a phone is typically not allowed in applications approved by the maker of a smart phone. *Id.* at col. 1:63-2:7.

22. Another conventional technique for identifying a mobile device prior to the Confirmetrics inventions was through a Subscriber Identity Module (SIM) card number. However, this number is usually accessible only by the cell network operator via the hardware layer of the phone. *See id.* at col. 2:8-14.

23. Conventional techniques for identifying mobile devices prior to the Confirmetrics inventions were easy to forge and identifying information would persist even if the phone changed ownership. They did not establish a link between the user of the phone and the phone itself. *Id.* at col. 1:64-2:23.

24. The Asserted Patents describe and claim inventions for identifying mobile devices using their configuration settings so that remote systems trust interacting with them more. *See id.* at col. 1:23-25 and col. 1:61-63.

25. The ’967, ’016, and ’048 Patent Specifications explain that extant authentication and security technologies “were not designed with mobile devices in mind.” ’016 Patent at col. 1:54-64. Traditional device fingerprinting methods and the attributes they collected and analyzed could not uniquely identify mobile devices. Even device identification techniques specific to mobile devices relied on

information that was either inaccessible or easily forged. *See* '016 Patent col. 2:4-31.

26. Confirmetrics' patents improve traditional device fingerprinting and identification technology by, for example, exploiting new types of information—unavailable outside the mobile device ecosystem—that can be collected from mobile devices via installed applications or SDKs. Specifically, the inventors state that the "advantage of [their] invention is that it uses a mobile device's configuration settings to uniquely identify it . . . so each mobile device will be found to be very different from every other." '016 Patent col. 3:8-13.

27. The inventors also recognized that, although a device's configuration settings are unlikely to change dramatically between interactions with a particular third party, variation is still inevitable, and can be accounted for by measuring the similarity between the configuration settings of devices being compared. This "fuzzy" matching improves device fingerprinting technology by increasing accuracy and reducing false-negatives due to inconsequential changes.

28. A person of ordinary skill in the art at the time of the invention would have recognized that the inventions claimed in the Asserted Patents were unconventional and described methods for uniquely identifying mobile devices using their configuration settings that was not routine at the time.

29. One of skill in the art would recognize that the subject matter claimed

in the Asserted Patent marks significant advancements over conventional mobile device identification techniques by relying on the mobile device configuration settings.

30. At the time of the invention, identifying mobile devices using their configuration settings was new and novel.

31. The subject matter claimed in the Asserted Patent represents a fundamental change in how mobile devices are identified and helps legitimate applications prove the identity of a mobile device to a third party.

32. A person of ordinary skill in the art at the time of the invention would have recognized that the method of collecting a multitude of configuration setting of a mobile device, processing this data, sending the processed data to a third party, and the third party comparing the received data with data received previously was not routine or conventional.

THE ’967 PATENT

33. Claim 1 of the ’967 Patent recites:

A method of identifying mobile electronic devices, comprising:

a. collecting a first plurality of configuration settings of a first mobile electronic device,

b. optionally summarizing, simplifying, and/or encoding the data of part a,

c. transmitting the result of part b to a third party,

d. collecting a second plurality of configuration settings of a second mobile electronic device which may or not be the same as said first mobile electronic device,

e. performing the same operation of part b on the data of part d,

f. transmitting the result of part e to said third party,

g. said third party calculating how similar the data received in part c is to the data received in part f, and

h. if, in part g, said third party determines said data received in part c is more than a threshold similar to said data received in part f, then determining that said first mobile electronic device is likely the same as said second mobile electronic device.

34. A person of ordinary skill in the art at the time of the invention would have understood that the claim element "collecting a first plurality of configuration settings of a first mobile electronic device" was not, at the time of the invention, conventional, well-understood, or routine.

35. A person of ordinary skill in the art at the time of the invention would have understood that the claim element "collecting a second plurality of configuration settings of a second mobile electronic device which may or not be the same as said first mobile electronic device" was not, at the time of the

invention, conventional, well-understood, or routine.

36. A person of ordinary skill in the art at the time of the invention would have understood that the combination of claim element "collecting a first plurality of configuration settings of a first mobile electronic device" and claim element "collecting a second plurality of configuration settings of a second mobile electronic device which may or not be the same as said first mobile electronic device" was not, at the time of the invention, conventional, well-understood, or routine.

37. A person of ordinary skill in the art at the time of the invention would have understood that the combination of elements in claim 1 of the '967 Patent was not, at the time of the invention, conventional, well-understood, or routine.

38. The novel use and arrangement of the specific combinations recited in claim 1 of the '967 Patent were not well-understood, routine, or conventional to a person skilled in the relevant field at the time of the inventions.

THE '016 PATENT

39. Claim 1 of the '016 Patent recites:

A device identification method, comprising:

a. receiving baseline configuration information indicative of a first plurality of mobile device configuration settings of a first mobile device;

b. receiving subsequent configuration information indicative of a second

plurality of mobile device configuration settings of a second mobile device;

c. determining a similarity between the subsequent configuration information and the baseline configuration information; and

d. responsive to detecting the similarity exceeding a threshold similarity, identifying the second mobile device as the first mobile device.

40. A person of ordinary skill in the art at the time of the invention would have understood that the claim element "receiving subsequent configuration information indicative of a second plurality of mobile device configuration settings of second mobile device" was not, at the time of the invention, conventional, well-understood, or routine.

41. A person of ordinary skill in the art at the time of the invention would have understood that the claim element "determining a similarity between the subsequent configuration information and the baseline configuration information" was not, at the time of the invention, conventional, well-understood, or routine.

42. A person of ordinary skill in the art at the time of the invention would have understood that the combination of claim element "receiving subsequent configuration information indicative of a second plurality of mobile device configuration settings of second mobile device" and claim element "determining a similarity between the subsequent configuration information and the baseline configuration information" was not, at the time of the invention, conventional,

well-understood, or routine.

43. A person of ordinary skill in the art at the time of the invention would have understood that the combination of elements in claim 1 of the ’016 Patent was not, at the time of the invention, conventional, well-understood, or routine.

44. The novel use and arrangement of the specific combinations recited in claim 1 of the ’016 Patent were not well-understood, routine, or conventional to a person skilled in the relevant field at the time of the inventions.

THE ’048 PATENT

45. Claim 1 of the ’048 Patent recites:

A device identification method, comprising:

a. receiving baseline configuration information indicative of a first plurality of mobile device configuration settings of a first mobile device and further indicative of at least one electronically accessible property of the first mobile device:

b. receiving subsequent configuration information indicative of a second plurality of mobile device configuration settings of a second mobile device and further indicative of at least one electronically accessible property of the second mobile device;

c. determining a similarity between the subsequent configuration information and the subsequent electronically accessible property information

of the second mobile device and the baseline configuration information and the baseline electronically accessible property information of the first mobile device; and

d. responsive to detecting the similarity exceeding a threshold similarity, identifying the second mobile device as the first mobile device.

46. A person of ordinary skill in the art at the time of the invention would have understood that the claim element "receiving baseline configuration information indicative of a first plurality of mobile device configuration settings of a first mobile device and further indicative of at least one electronically accessible property of the first mobile device" was not, at the time of the invention, conventional, well-understood, or routine.

47. A person of ordinary skill in the art at the time of the invention would have understood that the claim element "receiving subsequent configuration information indicative of a second plurality of mobile device configuration settings of a second mobile device and further indicative of at least one electronically accessible property of the second mobile device" was not, at the time of the invention, conventional, well-understood, or routine.

48. A person of ordinary skill in the art at the time of the invention would have understood that the combination of claim element "receiving baseline configuration information indicative of a first plurality of mobile device

configuration settings of a first mobile device and further indicative of at least one electronically accessible property of the first mobile device" and claim element "receiving subsequent configuration information indicative of a second plurality of mobile device configuration settings of a second mobile device and further indicative of at least one electronically accessible property of the second mobile device" was not, at the time of the invention, conventional, well-understood, or routine.

49. A person of ordinary skill in the art at the time of the invention would have understood that the combination of elements in claim 1 of the '048 Patent was not, at the time of the invention, conventional, well-understood, or routine.

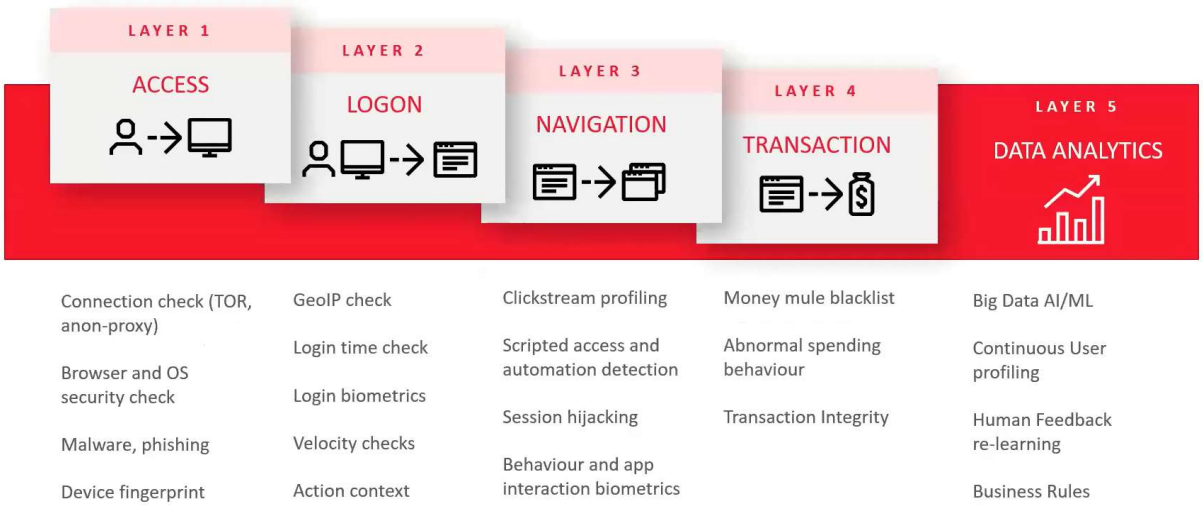
50. The novel use and arrangement of the specific combinations recited in claim 1 of the '048 Patent were not well-understood, routine, or conventional to a person skilled in the relevant field at the time of the inventions.

THREATMARK'S PRODUCTS

51. ThreatMark makes, imports, sells, offers to sell, distributes, licenses, markets, and/or uses ThreatMark fraud detection and prevention software (e.g., the ThreatMark Anti-Fraud Suite or "AFS," the ThreatMark software platform, SDK,

device client software, and the systems/methods employed by those applications ("The Accused Products").

52. ThreatMark Accused Products feature various layers security analysis.

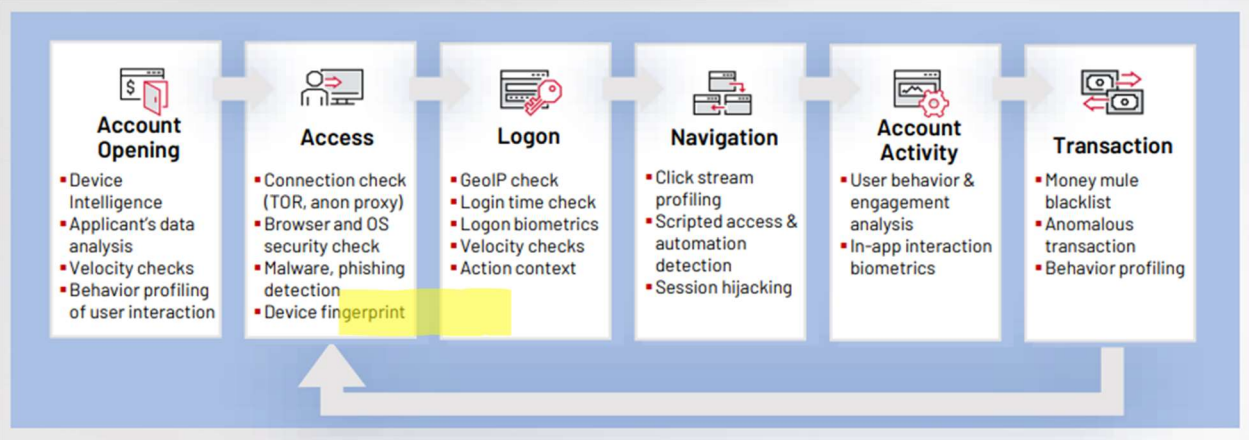


53. ThreatMark publishes accurate information about its products and services on its website (https://www.threatmark.com/).

54. ThreatMark uses JavaScript (for online user transactions) and an SDK (for device-borne transactions) for device intelligence and data gathering.

55. According to ThreatMark, its software provides a method for device identification by pulling a wide range of attributes to create high resolution device fingerprints utilizing unique data points.

56. ThreatMark identifies the devices of returning users by using device fingerprinting.



https://www.threatmark.com/dist/files/ThreatMark-AFS-Datasheet.pdf

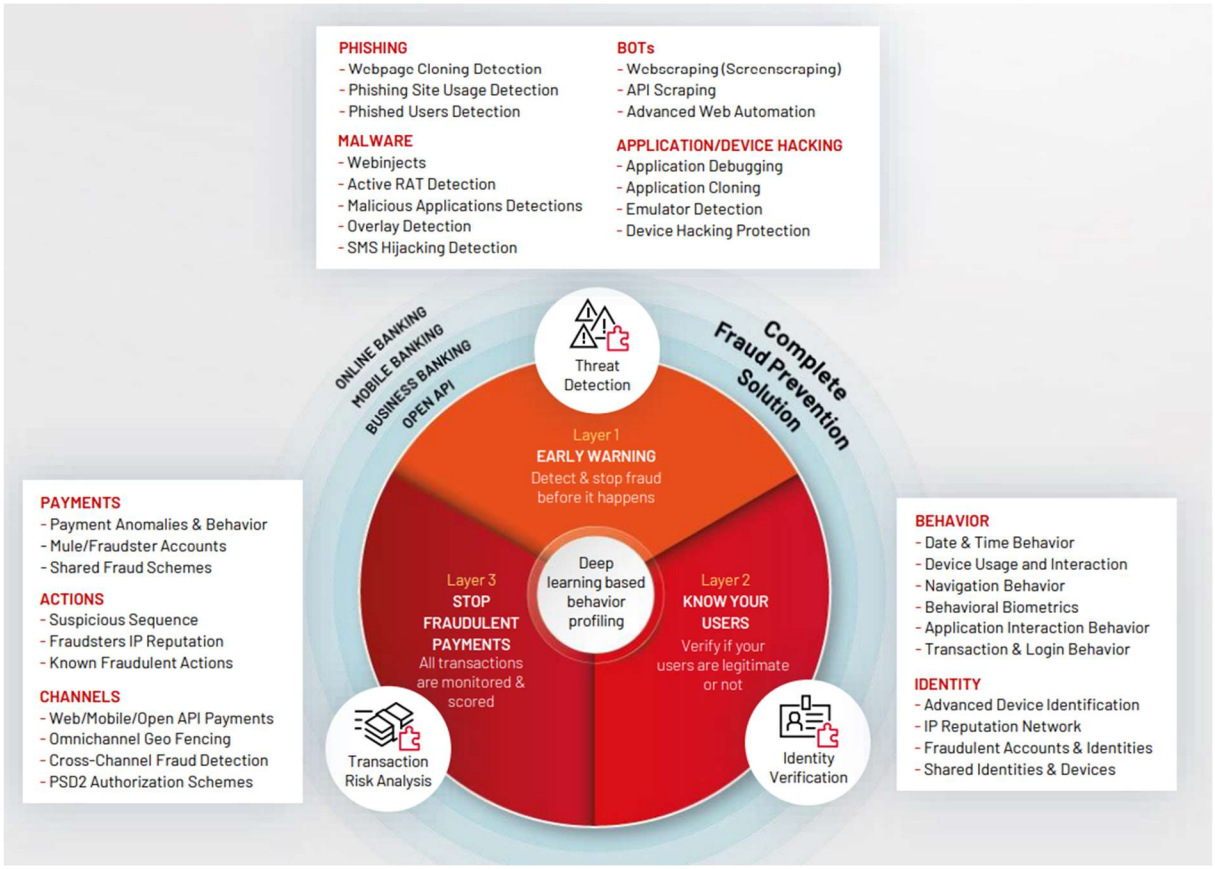
57. ThreatMark identifies devices of returning users and suspected fraudsters using device fingerprinting.

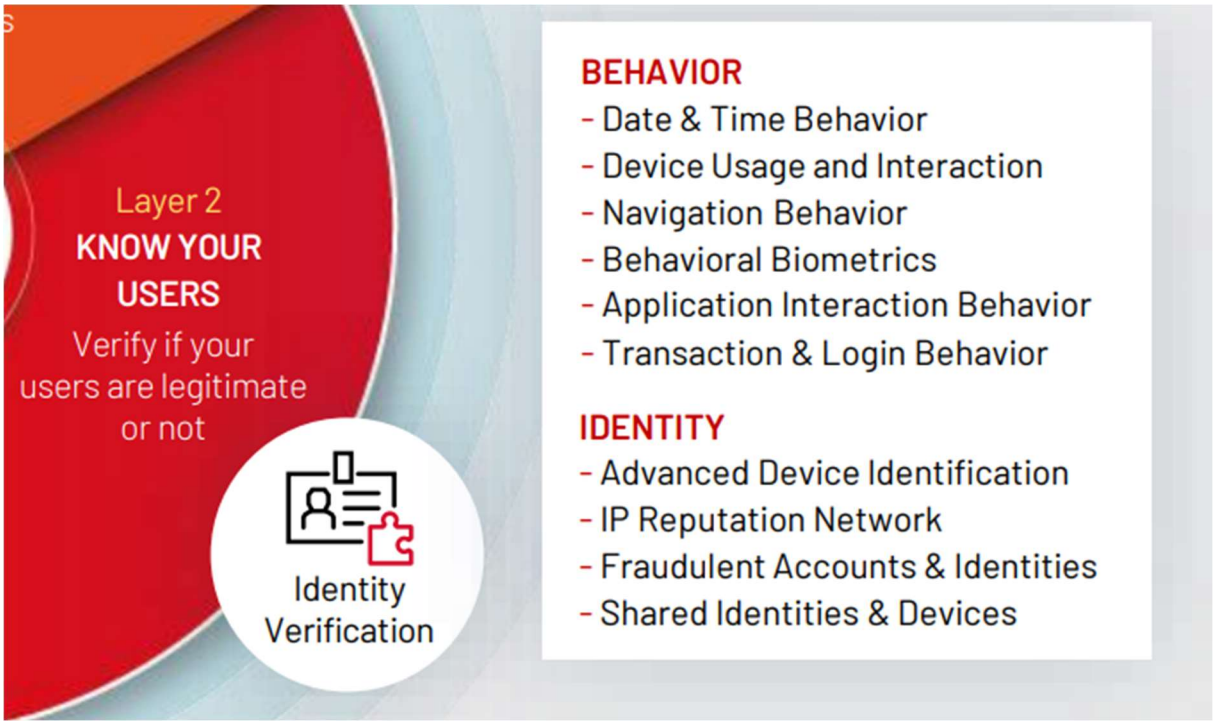
> ThreatMark keeps track of all users' devices used to access the internet banking application, including portable devices.

> Network categories include known blacklisted attacker networks, anonymous proxy and TOR, and also secure networks with a proven history. Access from suspicious networks with new IP addresses is considered risky. All this collected information together with many other parameters (browser language, resolution, available functions, etc.) form a unique device ID that is useful in detecting various attacks.

https://www.threatmark.com/dist/files/ThreatMark-PSD2-Whitepaper.pdf

58. ThreatMark collects user configuration settings including installed application data, application version information, data regarding device usage and interaction, and attributes that are not publicly known and maintained in secret by ThreatMark.





https://www.threatmark.com/dist/files/ThreatMark-PSD2-Whitepaper.pdf

59. In normal operation as intended by ThreatMark, the Accused Products (including software provided in ThreatMark's SDK and embedded in an iOS or Android device) collect configuration settings of the mobile device.

60. ThreatMark collects and analyzes data about configuration settings on user devices.

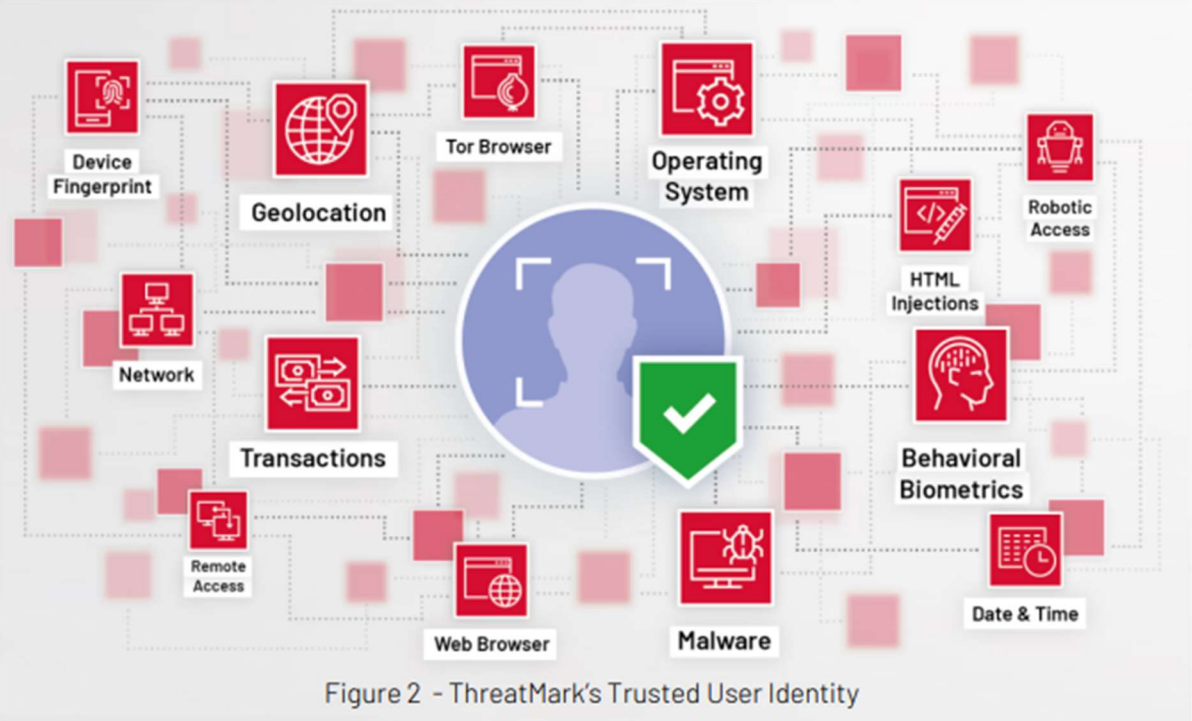


Figure 2 - ThreatMark's Trusted User Identity

https://www.threatmark.com/dist/files/ThreatMark-Fraud-Detection-Approach.pdf

61. ThreatMark validates more than 25 million users and over 1 billion logins and transactions yearly.

> At ThreatMark, we make sure that the entire digital journey (onboarding, authentication, account management, transactions...) is trusted and safe for both end-users and businesses. ThreatMark goes beyond the industry standards to validate more than 25 million users and over 1 billion logins and transactions yearly.

https://www.threatmark.com/dist/files/ThreatMark-PSD2-Whitepaper.pdf

62. ThreatMark provides a software service (*e.g.* ThreatMark Anti-Fraud Suite) accessible via its servers and SDK, to embed software code in applications and websites accessed via mobile devices.

63. ThreatMark's Anti-Fraud Suite (AFS) creates a trusted user profile consisting of mobile device configurations including installed applications, accessibility settings (e.g., overlay), permissions granted to applications, and OS modifications.

64. The device configuration settings are signals used to create a device fingerprint or user profile.

65. ThreatMark's AFS advertises a multi-layered approach including: (1) Threat Detection; (2) Identity Verification; and (3) Transaction Risk Analysis.

> ThreatMark Anti-Fraud Suite (AFS) is the most advanced fraud prevention solution, with a unique feature set & scope. Our comprehensive solution covers protections across the entire customer journey, through:
>
> **Layer 1 –** Threat Detection – early warning scope where threats are detected even before they make any damage
>
> **Layer 2 –** Identity Verification – where legitimate users are verified and fraudsters are denied
>
> **Layer 3 –** Transaction Risk Analysis – where all transactions are evaluated, monitored and scored

https://www.threatmark.com/why-threatmark/

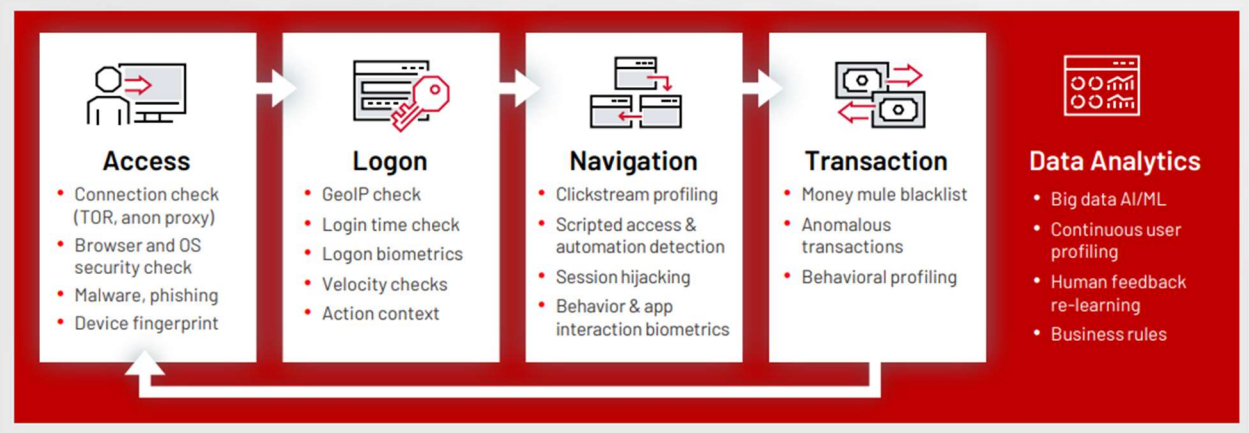
66. Embedded ThreatMark AFS code collects user configuration settings of a mobile device and sends that information to a server for analysis.

ThreatMark AFS comprises of the following components:

- **Analytics server**, deployed either on-premise or in the cloud. The analytics server processes data, applies machine learning algorithms, and hosts the web interface (for fraud analysts and security teams) and APIs (for integration with other systems, for example transaction scoring).
- **JavaScript probe**, a code running seamlessly inside each web session of protected users.
- **Mobile SDK** for Android and iOS, a library embedded into the protected application.
- **REST API**, scoring of login and transaction events.

https://www.threatmark.com/faq/

67. ThreatMark publishes the following image depicting the ThreatMark process:



https://www.threatmark.com/dist/files/ThreatMark-PSD2-Whitepaper.pdf

68. ThreatMark directs or controls the performance of collecting configuration information and transmission of such information to ThreatMark secure servers.

Protecting the Authentication & Authorization Portal

Each communication session in which the authentication data is transmitted must be protected against data capturing or manipulation by unauthorized parties (RTS Article 4, 3(c)).

https://www.threatmark.com/dist/files/ThreatMark-PSD2-Whitepaper.pdf

69. ThreatMark keeps track of all users' devices, including mobile devices.

ThreatMark keeps track of all users' devices used to access the internet banking application, including portable devices.

https://www.threatmark.com/dist/files/ThreatMark-PSD2-Whitepaper.pdf

70. ThreatMark receives configuration information from multiple devices to identify returning users.

We give banks the ability to recognize trusted returning clients and their devices by gathering all available data. Regardless of the platform and without any client-side agent, we detect insecure, compromised or infected devices. We analyze suspicious applications on them, installed plugins and the operation system status. In case of infection, the device can be automatically isolated from your secure environment, prevented from performing certain actions, and reported instantly for further investigation through centralized analytical interface.

https://www.threatmark.com/use-cases/endpoint-protection/

For each device, ThreatMark checks software components such as OS type and version, various frameworks types and versions (.NET), browser plugins (Flash, Java, Silverlight) including versions.

https://www.threatmark.com/dist/files/ThreatMark-PSD2-Whitepaper.pdf

> We go beyond evidence-based checks – we collect the thousand pieces of information that clients create during their sessions on their devices, connect them, analyze them, and get an extensive relevant output.

https://www.threatmark.com/use-cases/endpoint-protection/

71. ThreatMark uses machine learning to determine similarities between the attributes of an instant device and other devices in its database.

> All transactions are evaluated against various models. Each model includes a group of rules corresponding to a transaction type, the channel used, etc. However, ThreatMark detection does not rely on the rules only – it uses advanced machine learning with human feedback that can adapt to new fraudulent scenarios not covered by the rules.

https://www.threatmark.com/dist/files/ThreatMark-PSD2-Whitepaper.pdf

- A powerful machine learning-based engine that analyzes each payment operations and active transactions in real time.

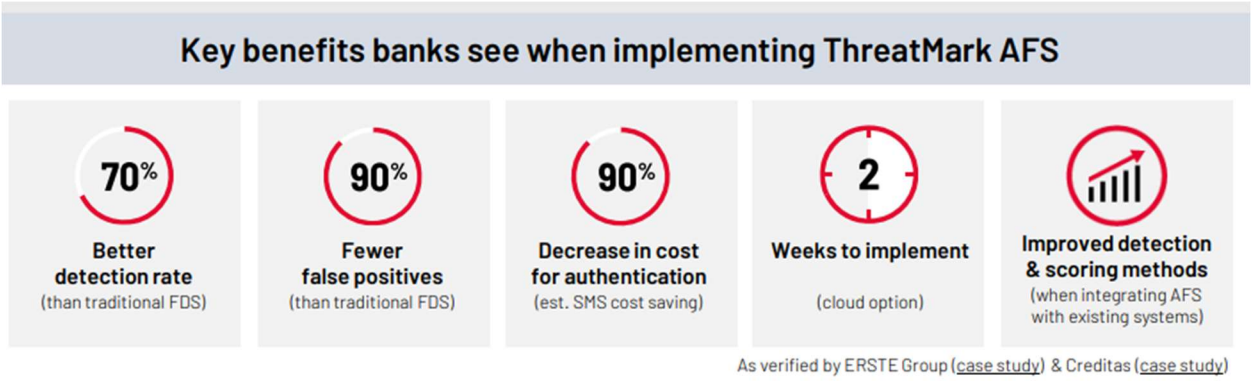
https://www.threatmark.com/products/anti-fraud-suite-afs/

72. ThreatMark claims that the AFS system is fully operational immediately after implementation for malware and phishing detections,.

> For malware and phishing detections, the system is fully operational immediately after implementation. For other threats, the modules need to go through a learning phase. Its length depends on the application type and operation size, typically ranging from two weeks to two months.

https://www.threatmark.com/faq/

73. ThreatMark advertises a decrease in false positives when using ThreatMark AFS.



https://www.threatmark.com/dist/files/ThreatMark-AFS-Datasheet.pdf

74. ThreatMark maintains that the user has the right to withdraw consent at any time and may have the right to object to ThreatMark's processing. *See* https://www.threatmark.com/privacy-terms/.

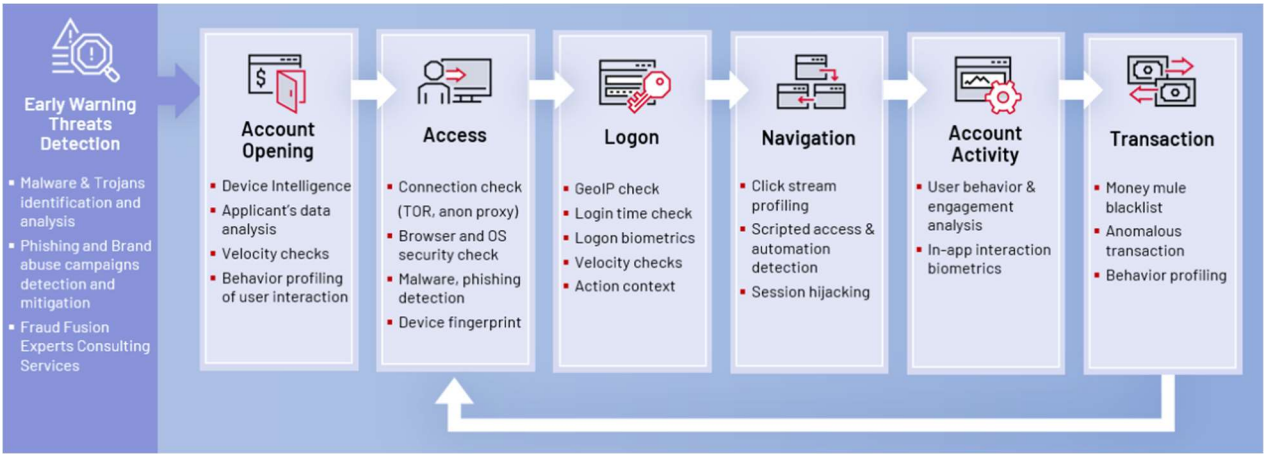
> **2. How do We collect your data**
>
> Regarding the grounds for processing your data, where we rely on your consent to process personal information, you have the right to withdraw your consent at any time, and where we rely on legitimate interests, you may have the right to object to our processing.

75. ThreatMark keeps any collected user data for five years after the initial collection.

> We will keep your data for 5 years after the initial collection. Once this time period has expired, we will delete your data; unless we obtained your consent with a longer storage or use or have a legal entitlement to store or use your data.

https://www.threatmark.com/privacy-terms/

76. ThreatMark publishes the following information about its device identification functionality:



https://www.threatmark.com/products/anti-fraud-suite-afs/

77. Each time a user visits a website or mobile app utilizing ThreatMark Accused Products, ThreatMark receives mobile device configuration settings corresponding to that user's device.

Insecure Mobile Device Configurations Detections

It is important to keep mobile devices secured the same way as desktop computers. ThreatMark can detect the following vulnerabilities:

- Outdated OS and applications versions
- Risky updates and other changes to the OS (rooted Android, jailbroken iOS)
- Insecure network usage
- Man-in-the-middle attacks – attempts to eavesdrop on the communication between a mobile application and a server
- Certificate issues during communication securing

https://www.threatmark.com/dist/files/ThreatMark-PSD2-Whitepaper.pdf

78. By comparing the received user configuration settings, ThreatMark can determine whether a mobile device in question is likely verifiable and authentic or fraudulent.

> Our solution continuously monitors behavior of a user and the devices they use. The information together serves as a proof of a user trustworthiness. We also use the ThreatMark user identity network intelligence to protect businesses through device identification, fingerprinting, honeypot technology, and location services. The service identifies returning customers even if they wipe cookies or use private browsing. It sets traps to detect malware in real time, and uses proxy piercing techniques to identify the true location and expose TOR networks or location spoofing.

https://www.threatmark.com/use-cases/endpoint-protection/

79. ThreatMark calculates a confidence score to measure a similarity between the attributes of an instant device to those of the devices in its database and identify returning devices where signals have changed.

80. The ThreatMark confidence score indicates whether each authentication step is performed by a legitimate user or an attacker.

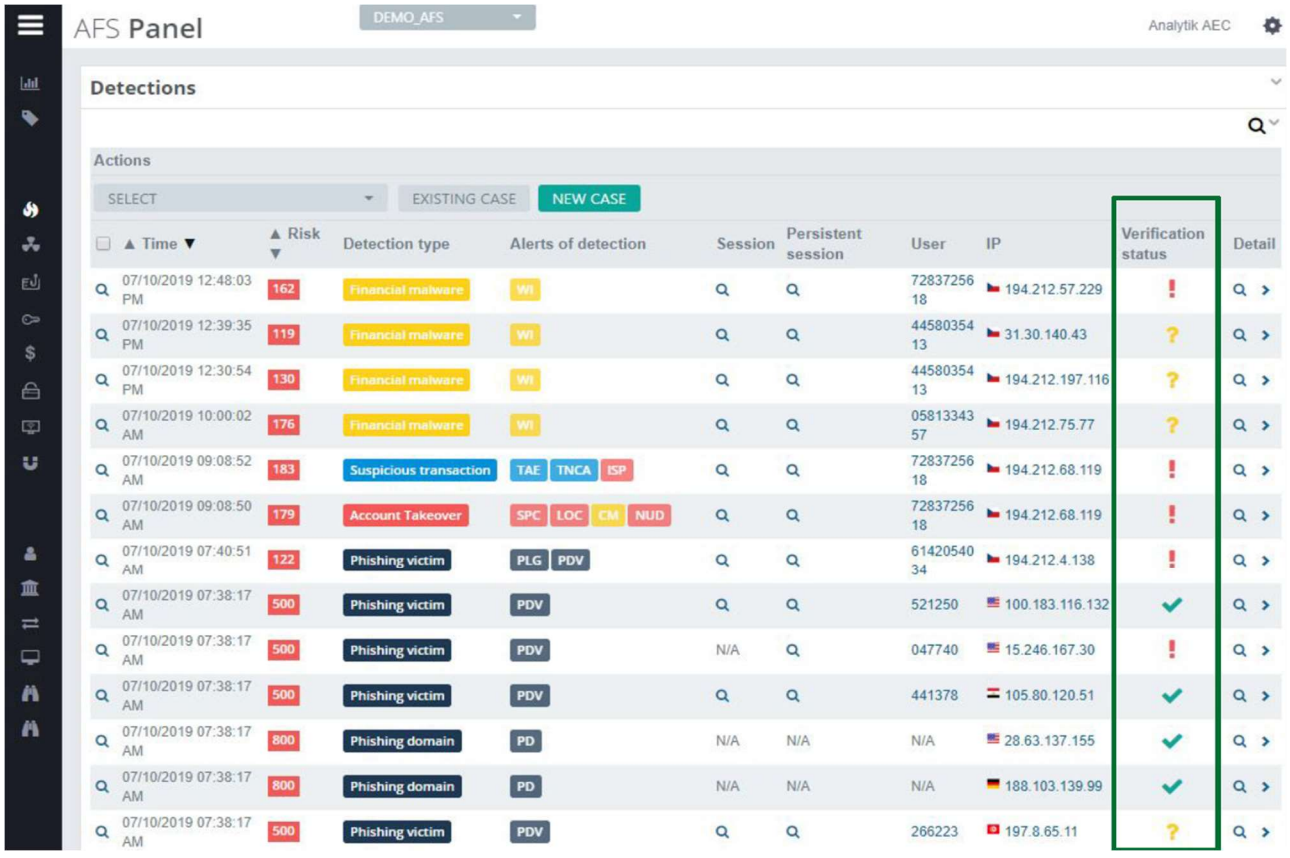
> The ThreatMark Solution gathers data about devices, user behavior, transactions and other contextual data across digital channels, and validates each event. It combines machine learning-based threat intelligence, transaction monitoring and behavioral biometrics to tell whether each authentication step or transaction is performed by a legitimate user or an attacker. Each event is scored in real time, and the score is used by the backend system to decide whether a user can be authenticated, a transaction authorized, or an additional factor should be required to validate the operation. As most users will be classified as legitimate, they will experience frictionless authentication and transaction authorization. The system will invoke strong authentication for high-risk logins and transactions only, meeting the PSD2 (Payment Services Directive) requirements. As a result, less than 15 % of logins will need to go through manual multi-factor authentication, which will reduce friction dramatically.

https://www.threatmark.com/use-cases/risk-based-strong-customer-authentication/

81. Where a device fails to meet set similarity thresholds, ThreatMark can require additional identification including two-factor (2FA) authentication before accepting requests from the visitor's device. ThreatMark's use of thresholds and user configuration settings reduces fraudulent activity without encumbering trusted visitors.

As most users will be classified as legitimate, they will experience frictionless authentication and transaction authorization. The system will invoke strong authentication for high-risk logins and transactions only, meeting the PSD2 (Payment Services Directive) requirements. As a result, less than 15 % of logins will need to go through manual multi-factor authentication, which will reduce friction dramatically.

https://www.threatmark.com/use-cases/risk-based-strong-customer-authentication/



https://www.threatmark.com/demo/

82. ThreatMark triggers additional authentication when a device does not meet threshold requirements. *See* https://www.threatmark.com/wp-content/uploads/2020/10/Success-Story-How-We-Enhanced-Security-UX-for-Slovenska-Sporitelna.pdf.

> With ThreatMark's adaptive user identification most users experience **frictionless authentication & seamless transaction authorization**. ThreatMark's system invokes strong authentication for high-risk logins and transactions only, meeting the necessary PSD2 requirements.
>
> As a result, less than **10% of logins would require manual multi-factor authentication**, which **reduces friction dramatically**. High-risk logins or transactions are directly denied.

If the Risk Score is low, the authentication element is not activated; when high, the authentication method (SMS) is escalated & sent.

83. In normal operation, the ThreatMark Accused Products summarize, simplify, and/or encode data, and transmit the data from a user's mobile device to a secure server for secure storage.

84. ThreatMark publishes the following information about how the Accused Products have been used to identify billions of users and allows users to skip two factor authentication and one time password more often, thus correctly identifying users with confidence on all devices.

> PSD2 states that the behavioral biometrics can be used as a independent authentication factor (inherence), so all users go through multi-factor strong customer authentication, but with minimal friction, as they only have to enter the first factor (typically login and password). The multiple factor authentication is augmented by passive behavioral biometrics, and the required level of security and user experience is kept.

https://www.threatmark.com/use-cases/risk-based-strong-customer-authentication/

85. ThreatMark's collected data is securely stored with third-party

providers.

86. ThreatMark's Privacy Policy is under regular review.

12. Changes to our privacy policy

We keep this Privacy Policy under regular review and places any updates on our web page. This Privacy Policy was last updated on November 25th, 2021.

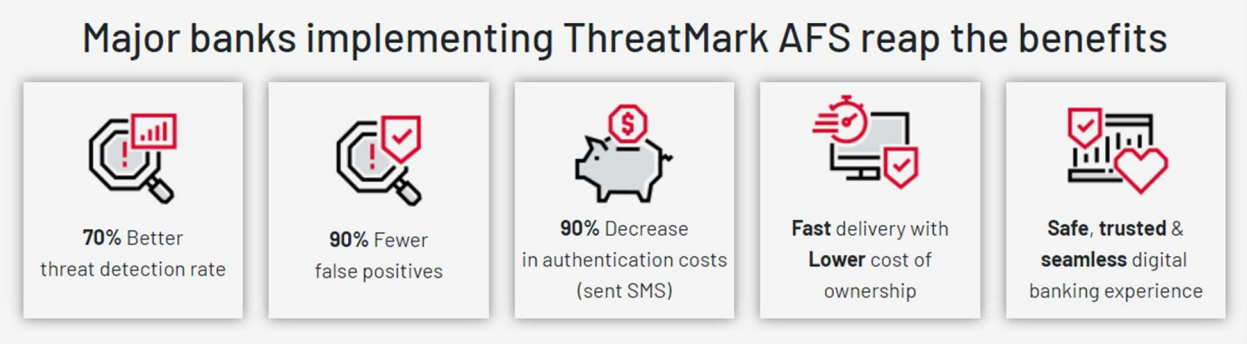
https://www.threatmark.com/privacy-terms/

87. ThreatMark publishes the following information about how the Accused Products provide valuable device identification for mobile and web and stop fraud, spam and account takeover with 99% less false positives using accurate device fingerprinting as a service (https://www.threatmark.com/demo/).

88. ThreatMark publishes the following information about how the Accused Products are trusted by public companies and banks, and how

ThreatMark's authentication system enhances security and user experience. *See* https://www.threatmark.com/why-threatmark/.

89. ThreatMark publishes the following information about how the high accuracy of the Accused Products saves banks money.



https://www.threatmark.com/why-threatmark/

> Strong and seamless authentication prevents account and session takeover, decreases friction by reducing the number of second factor authentication and authorization requests, and also saves money on SMS OTPs. Our case study shows that a bank with two million uses can save up to one million euro a year by implementing this adaptive authentication approach.

https://www.threatmark.com/use-cases/risk-based-strong-customer-authentication/

COUNT I: DIRECT INFRINGEMENT OF U.S. PATENT NO. 8,838,967

90. Confirmetrics re-alleges all preceding allegations as if set forth here.

91. Confirmetrics is the owner by assignment of all substantial rights, including the right to enforce and collect past and future royalties for infringement, in and to U.S. Patent No. 8,838,967 (the "'967 Patent") titled UNIQUELY IDENTIFYING A MOBILE ELECTRONIC DEVICE, which issued on September 16, 2014.

92. Exhibit A is a true and correct copy of the '967 Patent.

93. The '967 Patent is valid and enforceable.

94. The '967 Patent Specification (and the '016 and '048 Patent Specifications) explains that extant authentication and security technologies "were not designed with mobile devices in mind." '016 Patent at col. 1:54-64. Traditional device fingerprinting methods and the attributes they collected and analyzed could not uniquely identify mobile devices. Even device identification techniques specific to mobile devices relied on information that was either inaccessible or easily forged. *See* '016 Patent at col. 2:4-31.

95. Confirmetrics' patents improve traditional device fingerprinting and identification technology by, for example, exploiting new types of information—unavailable outside of the mobile device ecosystem—that can be collected from mobile devices via installed applications or SDKs. Specifically, the inventors state that the "advantage of [their] invention is that it uses a mobile device's configuration settings to uniquely identify it . . . so each mobile device will be found to be very different from every other." '016 Patent at col. 3:8-13.

96. Additionally, the inventors recognized that, although a device's configuration settings are unlikely to change dramatically between interactions with a particular third party, variation is still inevitable, and can be accounted for by measuring the similarity between the configuration settings of devices being

compared. This "fuzzy" matching also improves device fingerprinting technology by increasing accuracy and reducing false-negatives due to inconsequential changes.

97. Defendant has infringed, and continues to infringe, literally or through the doctrine of equivalents, one or more claims, including Claims 1-4, 7-9, 15, 16, and 19-21 of the '967 Patent under 35 U.S.C. § 271(a) by making, using, importing, selling, and/or offering for sale the Accused Products in the United States without authority.

98. Defendant encourages others, including its customers and users of its infringing software, to use the Accused Products in the United States without authority.

99. Defendant conditions its customers' receipt of ThreatMark's services upon the integration and/or incorporation of Defendants' software and scripts (e.g., in mobile application software) and dictates the manner and timing of performance (e.g., pursuant to the ThreatMark SDK) to direct and control the performance of processes that practice the subject matter claimed in the '967 Patent.

100. ThreatMark has been on notice of the '967 Patent and how it practices the claimed subject matter at least as early as this complaint.

101. Claim 1 of the '967 Patent recites:

A method of identifying mobile electronic devices, comprising:

a. collecting a first plurality of configuration settings of a first mobile electronic device,

b. optionally summarizing, simplifying, and/or encoding the data of part a,

c. transmitting the result of part b to a third party,

d. collecting a second plurality of configuration settings of a second mobile electronic device which may or not be the same as said first mobile electronic device,

e. performing the same operation of part b on the data of part d,

f. transmitting the result of part e to said third party,

g. said third party calculating how similar the data received in part c is to the data received in part f, and

h. if, in part g, said third party determines said data received in part c is more than a threshold similar to said data received in part f, then determining that said first mobile electronic device is likely the same as said second mobile electronic device.

102. As exemplified in the information referenced in the above paragraphs and the use of one or more of the Accused Products, ThreatMark performs and provides software for performing a method of identifying electronic devices that includes collecting data of a first plurality of configuration settings of a first mobile electronic device and optionally summarize, simplify, or encode the collected data

and transmit the data to a ThreatMark server for multiple mobile devices.

103. ThreatMark directs or controls its customers' performance of the methods claimed in the '967 Patent and conditions participation in and receipt of ThreatMark services upon performance of steps of the claimed methods, establishing the manner and timing of that performance by provision and requirement for incorporation of ThreatMark software or SDK in customer application software.

104. ThreatMark and its customers form a joint enterprise for practicing the device identification and authentication methods claimed in the '967 Patent.

105. ThreatMark servers determine the identification of the devices based on received data to determine if a mobile device is similar to another mobile device.

106. Defendant's infringing activities are and have been without authority or license under the '967 Patent.

107. Plaintiff is entitled to recover from Defendant the damages sustained by Plaintiff as a result of Defendant's infringing acts, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court, pursuant to 35 U.S.C. § 284.

COUNT II – INDIRECT PATENT INFRINGEMENT OF THE '967 PATENT

108. Confirmetrics realleges and incorporates by reference the allegations set forth above, as if set forth verbatim herein.

109. ThreatMark is liable for indirect infringement, literally or through the doctrine of equivalents, under 35 U.S.C. § 271(b) of one or more claims, including Claims 1, 2-4, 7-9, 15, 16, and 19-21 of the '967 Patent because it makes, uses, imports, sells, and/or offers for sale the Accused Products and knowingly encourages, aids, and directs others (e.g. customers) to use and operate the Accused Products in an infringing manner.

110. ThreatMark is also liable for indirect infringement, literally or through the doctrine of equivalents, under 35 U.S.C. § 271(c) of one or more claims, including Claims 1, 2-4, 7-9, 15, 16, and 19-21 of the '967 Patent because it makes, uses, imports, sells, and/or offers for sale the ThreatMark Accused Products and knowingly encourages, aids, and directs others (e.g. customers) to use and operate the Accused Products in an infringing manner. ThreatMark has engaged in these activities knowing that the Accused Products are especially made and adapted for use, and in fact used, in a manner that constitutes infringement of the '967 Patent. The Accused Products constitute material parts of the patented inventions of the '967 Patent and are not staple articles of commerce suitable for substantial non-infringing uses.

111. ThreatMark specifically intends the Accused Products to be used and operated to infringe at least one or more claims of the ’967 Patent.

112. ThreatMark encourages, directs, aids, and abets the installation, configuration, and/or usage of the Accused Products in an infringing manner in the United States without authority or license.

113. ThreatMark has instructed its customers to use the Accused Products in an infringing manner.

114. Confirmetrics is entitled to recover from ThreatMark the damages sustained as a result of ThreatMark’s infringing acts 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, pursuant to 35 U.S.C. § 284.

COUNT III: DIRECT INFRINGEMENT OF U.S. PATENT NO. 9,603,016

115. Confirmetrics re-alleges all preceding allegations as set forth here.

116. Confirmetrics is the owner by assignment of all substantial rights, including the right to enforce and collect past and future royalties for infringement, in and to U.S. Patent No. 9,603,016 (the “’016 Patent”), titled UNIQUELY IDENTIFYING A MOBILE ELECTRONIC DEVICE, which issued on March 21, 2017.

117. Exhibit B is a true and correct copy of the ’016 Patent.

118. The ’016 Patent is valid and enforceable.

119. Defendant has infringed, and continues to infringe, literally or through the doctrine of equivalents, one or more claims, including Claims 1-5, 8, 12, 13, 14, 17, and 20 of the ’016 Patent under 35 U.S.C. § 271(a) by making, using, importing, selling, and/or offering for sale the Accused Products in the United States without authority.

120. Defendant encourages others, including its customers and users of its infringing software to use the Accused Products in the United States without authority.

121. Claim 1 of the ’016 Patent recites:

A device identification method, comprising:

a. receiving baseline configuration information indicative of a first plurality of mobile device configuration settings of a first mobile device;

b. receiving subsequent configuration information indicative of a second plurality of mobile device configuration settings of a second mobile device;

c. determining a similarity between the subsequent configuration information and the baseline configuration information; and

d. responsive to detecting the similarity exceeding a threshold similarity, identifying the second mobile device as the first mobile device.

122. As exemplified in the information referenced in the above paragraphs

and the use of one or more of the Accused Instrumentalities, the Accused Instrumentalities provide a method of identifying electronic devices. The method includes receiving for multiple mobile devices, baseline configuration information, which is indicative of a mobile device configuration settings and indicative of an electronically accessible property of the mobile device.

123. ThreatMark servers determine the identification of the devices based on the received configuration information to determine if a mobile device is similar to another mobile device.

124. Defendant's infringing activities are and have been without authority or license under the '016 Patent.

125. Plaintiff is entitled to recover from Defendant the damages sustained by Plaintiff as a result of Defendant's infringing acts, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court, pursuant to 35 U.S.C. § 284.

COUNT IV: INDIRECT INFRINGEMENT OF U.S. PATENT NO. 9,603,016

126. Confirmetrics realleges and incorporates by reference the allegations set forth above, as if set forth verbatim herein.

127. ThreatMark is liable for indirect infringement, literally or through the doctrine of equivalents, under 35 U.S.C. § 271(b) of one or more of claims, including Claims 1-5, 8, 12, 13, 14, 17, and 20 of the '016 Patent because it makes,

uses, imports, sells, and/or offers for sale the Accused Products and knowingly encourages, aids, and directs others (e.g. customers) to use and operate the Accused Products in an infringing manner.

128. ThreatMark is also liable for indirect infringement, literally or through the doctrine of equivalents, under 35 U.S.C. § 271(c) of one or more claims, including Claims 1-5, 8, 12, 13, 14, 17, and 20 of the ’016 Patent because it makes, uses, imports, sells, and/or offers for sale the Accused Products and knowingly encourages, aids, and directs others (e.g. customers) to use and operate the Accused Products in an infringing manner. ThreatMark has engaged in these activities knowing that the Accused Products are especially made and adapted for use, and in fact used, in a manner that constitutes infringement of the ’016 Patent. The Accused Products constitute material parts of the patented inventions of the ’016 Patent, and are not staple articles of commerce suitable for substantial non-infringing uses.

129. ThreatMark specifically intends the Accused Products to be used and operated to infringe at least one or more claims of the ’016 Patent.

130. ThreatMark encourages, directs, aids, and abets the use, configuration, and installation of the Accused Products.

131. ThreatMark has instructed its customers to use the Accused Products in an infringing manner.

132. Confirmetrics is entitled to recover from ThreatMark the damages sustained as a result of ThreatMark's infringing acts 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, pursuant to 35 U.S.C. § 284.

COUNT V: DIRECT INFRINGEMENT OF U.S. PATENT NO. 9,801,048

133. Plaintiff re-alleges the preceding allegations as if set forth here.

134. Confirmetrics is the owner by assignment of all substantial rights, including the right to enforce and collect past and future royalties for infringement, in and to U.S. Patent No. 9,801,048 (the "'048 Patent") titled UNIQUELY IDENTIFYING A MOBILE ELECTRONIC DEVICE, which issued on October 24, 2017.

135. Exhibit C is a true and correct copy of the '048 Patent.

136. The '048 Patent is valid and enforceable

137. ThreatMark has infringed, and continues to infringe, literally or through the doctrine of equivalents, one or more claims, including Claims 1-3, 5, 8, 12, 13, 14, 17, and 20 of the '048 Patent under 35 U.S.C. § 271(a) by making, using, importing, selling, and/or offering for sale the Accused Products in the United States without authority.

138. Defendant encourages others, including its customers and users of its infringing software to use the Accused Products in the United States without

authority.

139. Claim 1 of the ’048 Patent recites:

A device identification method, comprising:

a. receiving baseline configuration information indicative of a first plurality of mobile device configuration settings of a first mobile device and further indicative of at least one electronically accessible property of the first mobile device;

b. receiving subsequent configuration information indicative of a second plurality of mobile device configuration settings of a second mobile device and further indicative of at least one electronically accessible property of the second mobile device;

c. determining a similarity between the subsequent configuration information and the subsequent electronically accessible property information of the second mobile device and the baseline configuration information and the baseline electronically accessible property information of the first mobile device; and

d. responsive to detecting the similarity exceeding a threshold similarity, identifying the second mobile device as the first mobile device.

140. As exemplified in the information referenced in the above paragraphs and the use of one or more of the Accused Products, the Accused Products provide

a method of identifying electronic devices. The method includes receiving for multiple mobile devices, baseline configuration information, which is indicative of a mobile device configuration settings and indicative of an electronically accessible property of the mobile device.

141. ThreatMark servers determine the identification of the devices based on the received configuration information to determine if a mobile device is similar to another mobile device.

142. Defendant's infringing activities are and have been without authority or license under the '048 Patent.

143. Plaintiff is entitled to recover from Defendant the damages sustained by Plaintiff as a result of Defendant's infringing acts, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court, pursuant to 35 U.S.C. § 284.

COUNT VI: INDIRECT INFRINGEMENT OF U.S. PATENT NO. 9,801,048

144. Confirmetrics realleges and incorporates by reference the allegations set forth above, as if set forth verbatim herein.

145. ThreatMark is liable for indirect infringement, literally or through the doctrine of equivalents, under 35 U.S.C. § 271(b) of one or more of claims, including Claims 1-3, 5, 8, 12, 13, 14, 17, and 20 of the '048 Patent because it makes, uses, imports, sells, and/or offers for sale the Accused Products and

knowingly encourages, aids, and directs others (e.g. customers) to use and operate the Accused Products in an infringing manner.

146. ThreatMark is also liable for indirect infringement, literally or through the doctrine of equivalents, under 35 U.S.C. § 271(c) of one or more claims, including Claims 1-3, 5, 8, 12, 13, 14, 17, and 20 of the '048 Patent because it makes, uses, imports, sells, and/or offers for sale the Accused Products and knowingly encourages, aids, and directs others (e.g. customers) to use and operate the Accused Products in an infringing manner. ThreatMark has engaged in these activities knowing that the Accused Products are especially made and adapted for use, and in fact used, in a manner that constitutes infringement of the '048 Patent. The Accused Products constitute material parts of the patented inventions of the '048 Patent, and are not staple articles of commerce suitable for substantial non-infringing uses.

147. ThreatMark specifically intends the Accused Products to be used and operated to infringe at least one or more claims of the '048 Patent.

148. ThreatMark encourages, directs, aids, and abets the use, configuration, and installation of the Accused Products.

149. ThreatMark has instructed its customers to use the Accused Products in an infringing manner.

150. Confirmetrics is entitled to recover from ThreatMark the damages as a

result of ThreatMark's infringing acts 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, pursuant to 35 U.S.C. § 284.

NOTICE OF REQUIREMENT OF LITIGATION HOLD

151. ThreatMark is hereby notified it is legally obligated to locate, preserve, and maintain all records, notes, drawings, documents, data, communications, materials, electronic recordings, audio/video/photographic recordings, and digital files, including edited and unedited or "raw" source material, and other information and tangible things that ThreatMark knows, or reasonably should know, may be relevant to actual or potential claims, counterclaims, defenses, and/or damages by any party or potential party in this lawsuit, whether created or residing in hard copy form or in the form of electronically stored information (hereafter collectively referred to as "Potential Evidence").

152. As used above, the phrase "electronically stored information" includes without limitation: computer files (and file fragments), e-mail (both sent and received, whether internally or externally), information concerning e-mail (including but not limited to logs of e-mail history and usage, header information, and deleted but recoverable e-mails), text files (including drafts, revisions, and active or deleted word processing documents), instant messages, audio recordings

and files, video footage and files, audio files, photographic footage and files, spreadsheets, databases, calendars, telephone logs, contact manager information, internet usage files, and all other information created, received, or maintained on any and all electronic and/or digital forms, sources and media, including, without limitation, any and all hard disks, removable media, peripheral computer or electronic storage devices, laptop computers, mobile phones, personal data assistant devices, Blackberry devices, iPhones, video cameras and still cameras, and any and all other locations where electronic data is stored. These sources may also include any personal electronic, digital, and storage devices of any and all of ThreatMark's agents, resellers, or employees if ThreatMark's electronically stored information resides there.

153. ThreatMark is hereby further notified and forewarned that any alteration, destruction, negligent loss, or unavailability, by act or omission, of any Potential Evidence may result in damages or a legal presumption by the Court and/or jury that the Potential Evidence is not favorable to ThreatMark's claims and/or defenses. To avoid such a result, ThreatMark's preservation duties include, but are not limited to, the requirement that ThreatMark immediately notify its agents and employees to halt and/or supervise the auto-delete functions of ThreatMark's electronic systems and refrain from deleting Potential Evidence, either manually or through a policy of periodic deletion.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests the Court enter judgment against Defendant and its subsidiaries, affiliates, officers, directors, agents, servants, employees and all persons in active concert or participation with them, granting the following relief:

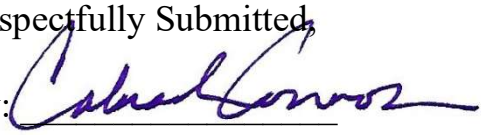
1. declaring that the Defendant has infringed the '967, '016, and '048 Patents;
2. awarding Plaintiff its damages suffered as a result of Defendant's infringement of the '967, '016, and '048 Patents;
3. awarding Plaintiff its costs, attorneys' fees, expenses, and prejudgment and post-judgment interest; and
4. granting Plaintiff such further relief as the Court deems just and proper.

JURY DEMAND

Plaintiff hereby demands a trial by jury of all issues so triable pursuant to Fed. R. Civ. P. 38.

Dated: December 16, 2022

Respectfully Submitted,

By: 

Cabrach J. Connor
TX State Bar No. 24036390
Email:Cab@CLandS.com
Jennifer Tatum Lee
TX State Bar No. 24046950

Email: Jennifer@CLandS.com
John M. Shumaker
TX State Bar No. 24033069
Email: John@CLandS.com
CONNOR LEE & SHUMAKER PLLC
609 Castle Ridge Road, Suite 450
Austin, Texas 78746
512.777.1254 Telephone
888.387.1134 Facsimile

ATTORNEYS FOR PLAINTIFF