

**Clarkson Law Firm, P.C.**  
Ryan J. Clarkson (SBN 257074)  
rclarkson@clarksonlawfirm.com  
Yana Hart (SBN 306499)  
yhart@clarksonlawfirm.com  
Bryan P. Thompson (SBN 354683)  
bthompson@clarksonlawfirm.com  
22525 Pacific Coast Highway  
Malibu, CA 90265  
Telephone: (213) 788-4050  
Fax: (213) 788-4070

**ALMEIDA LAW GROUP**  
Matthew J. Langley (SBN 342846)  
matt@almeidawgroup.com  
849 W. Webster Avenue  
Chicago, Illinois 60614  
Telephone: (773) 554-9354

*Court-Appointed Class Counsel*

**SUPERIOR COURT OF THE STATE OF CALIFORNIA  
COUNTY OF MARIN**

JOHN DOE I, JOHN DOE II, AND JOHN DOE )  
III, individually and on behalf of all others )  
similarly situated, )  
Plaintiffs, )  
vs. )  
MARIN HEALTH MEDICAL CENTER, )  
Defendant. )

Case No.: CV0002218

[Case Assigned for All Purposes to the  
Hon. Stephen P. Freccero in Courtroom A]

**DECLARATION OF BRYAN HELLER IN  
SUPPORT OF PLAINTIFFS' UNOPPOSED  
MOTION FOR FINAL APPROVAL OF  
THE CLASS ACTION SETTLEMENT**

1 I, Bryan Heller, do hereby declare and state as follows:

2 1. I am a Co-Founding partner and the Chief Operating Officer of ClaimScore, LLC  
3 (“ClaimScore”), a legal technology company that, among other things, provides complex data  
4 analysis and pattern recognition services that assist claims administrators in identifying fraudulent  
5 claims in class action settlements. ClaimScore has been retained by the court-appointed administrator  
6 Verita Global, LLC (“Verita”) to analyze the claims collected in the above-referenced class action  
7 (the “MarinHealth Settlement”) for evidence of fraud. The following statements are based on my  
8 personal knowledge and information provided by other ClaimScore principals and employees  
9 working under my supervision, and if called upon to do so, I could and would testify competently  
10 about these issues.  
11

12 **I. Executive Summary of Claim Validation Results**

13 2. The MarinHealth Settlement involves Defendant MarinHealth Medical Center’s  
14 alleged use of Meta Pixel on its Websites between August 1, 2019, and May 27, 2025, during which  
15 Plaintiffs allege their web usage data, containing Personal Information, was shared with third parties,  
16 allegedly resulting in the invasion of Plaintiffs’ and Settlement Class Members’ privacy. Because the  
17 parties did not have contact information for all potential class members, there was an “indirect notice”  
18 component to the settlement that required purported class members to fill out a basic claim form in  
19 order to receive a monetary payment. These types of settlements – with low barriers for unknown  
20 parties to receive a settlement payment – are ripe targets for fraudulent actors and organizations to  
21 attempt to engage in large-scale technological fraud (which we refer to as “programmatic fraud”).  
22 This Declaration is limited to our review and analysis of the claims that were submitted in this case  
23 prior to August 19, 2025 9:54:14 PM PT but excluding the 1,109 claims where the claim’s telephone  
24 numbers were dropped when Verita exported the claims data from their claims management system  
25 prior to transferring the claims data to ClaimScore..  
26  
27  
28

3. I have personally witnessed rampant claims fraud in class actions similar to the MarinHealth Settlement. I have personally observed an increase in the amount of programmatic fraud in recent years. Fraudsters are steadily improving upon the sophistication of their fraudulent methods. Based on the sophistication of what I have seen in those cases and in this case, it is likely that this fraud is being perpetrated by organized entities, some of which are international.

4. Simple, rule-based fraud detection methodologies (known as “group and slash” and as detailed in paragraphs 36 below) are meaningfully flawed and when they’re the only line of defense against fraud, a substantial number of fraudulent claims are paid. The use of Expert System AI and pattern recognition technology to eliminate fraud is critical in achieving maximum accuracy. ClaimScore’s technology aligns with the leading fraud detection technology used across other markets (e.g. FinTech, Traditional Banking, eCommerce, etc.); however, it was purpose built for the detection of fraud in class action and other collective litigation settlements.

5. To date, ClaimScore has analyzed the MarinHealth Settlement claims received prior to August 19, 2025 at 9:54:14 p.m. PT, excluding the 1,109 claims where the claim's telephone numbers were dropped when Verita exported the claims data from their claims management system prior to transferring the claims data to ClaimScore. ClaimScore will subsequently review these 1,109 claims as well as all other claims received for this settlement through the close of the claims period. An update to this declaration will be filed upon completion of the final analysis of all claims to provide the Court with the final claim review results.

6. Based on our findings from the previously reviewed claims, 60,528 claims exhibited substantial evidence of fraud and were recommended to be “Rejected,” 1,895 claims did not exhibit substantial evidence of fraud and were recommended to be “Approved”. For purposes of this Declaration, “Approved” means that the claim, as submitted, did not present as fraudulent under

1 ClaimScore’s analysis and is recommended to the Settlement Administrator for final review and  
2 determination in the context of the Settlement as a whole. Each claim, regardless of its determination  
3 (e.g., “Rejected” or “Approved”), has been tagged with a series of deduction codes (when applicable)  
4 to indicate what evidence caused the claim’s score to be reduced and ultimately resulted in its  
5 determination. The percentage of fraudulent and valid claims observed in this case were on par with  
6 the levels of fraud ClaimScore has observed in similar cases.  
7

## 8 **II. ClaimScore’s Background and Experience**

9 7. The ClaimScore team has over 40 years of class action case experience, and includes  
10 both class action attorneys, individuals with class action claim administration experience, data  
11 analysts, and a full software development team. Our founders have represented litigants on both sides  
12 of consumer (and other) class actions and have administered numerous cases in state and federal  
13 courts throughout the United States.  
14

15 8. ClaimScore was developed, specifically based on its founders’ education and  
16 expertise, to review and validate claims in class action settlements, individually and in real-time or  
17 retroactively, based on objective criteria that are applied consistently and uniformly to all people  
18 making claims in these settlements.

19 9. ClaimScore’s technical team consists of fifteen (15) full-time professionals led by a  
20 veteran AI systems architect with over a decade of experience. The team includes seven (7) software  
21 engineers, each with a background in Systems Engineering and a combined 40+ years of experience  
22 developing artificial intelligence technologies. Two of these engineers hold advanced degrees – one  
23 in Big Data and Machine Learning, and the other in Systems Management. The engineering team is  
24 supported by four additional developers, one with a degree in Systems Engineering, two with degrees  
25 in Mathematics, one of whom is currently pursuing an advanced degree in Big Data and Machine  
26 Learning and the fourth currently pursuing a degree in Systems Engineering. In addition, ClaimScore  
27  
28

1 employs two senior DevOps engineers with over eighteen (18) years of combined experience  
2 designing and maintaining scalable cloud infrastructure for AI systems, as well as a dedicated VP of  
3 Operations and Product with nearly a decade of experience managing data analytics and AI products.

4         10. ClaimScore is a legal technology company that assists with the administration of class  
5 actions, and, in particular, provides complex data analysis and pattern recognition services to review  
6 and assess claims made in the settlement of class actions to determine whether those claims are valid  
7 or fraudulent. ClaimScore is the only independent software solution that provides such services to  
8 the class action industry. ClaimScore’s fraud detection technology has been used in more than 30  
9 large-scale class action settlements – both federal and state – over the past two (2) years.

### 11 **III. The Evolution of Claim Fraud**

12         11. Fraudulent claim submissions have existed for decades, but the scale and  
13 sophistication of such activity have evolved dramatically with advances in digital communication.  
14 The earliest forms of fraud, at scale, emerged during the industry’s transition from print-based notice  
15 campaigns to digital advertising on the internet. Social media platforms, online forums, and blogs  
16 became effective tools for notifying potential class members—but they also created new vectors for  
17 abuse, with users publicly sharing instructions on how to file class action claims for settlements they  
18 were not necessarily eligible to participate in. This also coincided with the availability of online claim  
19 forms, which made it easier than ever for fraudulent submissions to be filed at scale with minimal  
20 friction.  
21

22         12. Early digital-era fraud was largely driven by “serial submitters”—individuals who  
23 routinely filed claims in every available settlement regardless of eligibility. These actors often  
24 submitted multiple claims per case using alternate version of their own contact information or contact  
25 information of their relatives, such as addresses, emails or phone numbers. This activity initially  
26 escaped detection, as the volume was low and these claims were not easily distinguishable from  
27

1 genuine claims.

2       13. By the late 2010s, however, fraud methods had become programmatic. In this phase,  
3 individuals and organized groups reverse-engineered the structure of online claim forms and  
4 developed scripts to automate submissions at massive scale. These automated submission tools,  
5 commonly referred to as “bots,” enabled bad actors to submit tens or even hundreds of thousands of  
6 claims per case. Unlike traditional internet bots used to scrape data or generate web traffic, these bots  
7 were created explicitly to extract funds from class action settlement programs.  
8

9       14. In response to growing concerns across the internet about automated abuse,  
10 technologies such as CAPTCHA and Web Application Firewalls (WAFs) were introduced to detect  
11 and block bots. Settlement administrators began deploying these tools to mitigate programmatic fraud  
12 in the class action context.  
13

14       15. As those countermeasures gained traction, fraud tactics once again evolved. A new  
15 wave of attacks leveraged “phone farms”—large clusters of physical mobile devices controlled  
16 through centralized software. These devices allowed fraudsters to rotate IP addresses, spoof unique  
17 device signatures, and simulate real user interactions. Because phone farms mimic legitimate mobile  
18 traffic, they are capable of bypassing conventional bot-detection systems and submitting high  
19 volumes of fraudulent claims without detection.  
20

21       16. Early iterations of programmatic and phone farm fraud primarily involved fake  
22 identities. Fraudsters used invented names, addresses, phone numbers, and emails, often relying on  
23 tools that can mass-produce or manage digital contact information. Payouts were then directed to  
24 fraud-controlled mobile numbers or email accounts to receive digital payments. While many cases  
25 involved digital payouts, some operations also employed check interception techniques to extract  
26 funds via traditional mail.  
27

28       17. As fraud detection tools became more effective in identifying fake identities, fraud

1 operations adapted once again, this time through the use of synthetic identities. Synthetic fraud  
2 involves blending real personal information, either purchased from illicit sources or scraped from  
3 public directories, with alternate contact details under the fraudster's control. Detecting synthetic  
4 identities requires advanced, domain-specific analysis capable of identifying subtle inconsistencies  
5 across multiple data points. ClaimScore is the only known fraud detection system purpose-built to  
6 detect complex submission fraud, including synthetic identity fraud, within the class action settlement  
7 ecosystem.  
8

#### 9 **IV. ClaimScore's Experience and Fraud Detection Methodology**

10 18. ClaimScore has extensive experience – and a particular expertise – in providing anti-  
11 fraud solutions to identify and exclude programmatic fraud from class action settlements like in the  
12 MarinHealth Settlement.  
13

14 19. ClaimScore has been named as the anti-fraud solution in numerous state and federal  
15 court class action settlements (in both the United States and Canada), including those with class  
16 payments exceeding \$100,000,000.00. We have worked alongside many of the claims administrators  
17 in the class action space, including A.B. Data Ltd., Digital Settlement, Angeion Group, Epiq Systems,  
18 Verita, American Legal Claims Services, EisnerAmper, Atticus Administration, Fidexis and others,  
19 reviewing more than 150,000,000 claims over the past year. We have been retained to provide a fraud  
20 analysis at the outset of matters, while matters are pending, and at the end of matters (when all of the  
21 claims have already been submitted for review).  
22

23 20. Here is a sample of currently active or recently finalized class action settlements in  
24 which ClaimScore was retained:

Case Name	Case Number	Court
Perez v. Rash Curtis & Associates	4:16-cv-03396-YGR	United States District Court for the Northern District of California
Rosenfeld et al. v AC2T, Inc.	506882/2023	New York Supreme Court for Kings County

Wyland v. Woopla	2023-CI-00356	Kentucky Circuit Court for Henderson County
Whiting v. Yellow Social Interactive Ltd.	2023-CI-00358	Kentucky Circuit Court for Henderson County
O'Malley, et al. v. FloSports, Inc.,	3:22-cv-04920JSC	United States District Court for the Northern District of California
Gunaratna v. Dr. Dennis Gross Skincare, LLC	1:23-CV-01967-ER	United States District Court for the Southern District of New York
Danielle Skarpnes v. Elixir Cosmetics OPCO LLC	CU23-04638	Superior Court of California, County of Solano
Lipsky, et al. v. American Behavioral Research Institute, LLC, d/b/a Relaxium	50-2023-CA-011526-XXXX-MB	Circuit Court of the Fifteenth Judicial Circuit in and for Palm Beach County, Florida
Jimenez v. Artsana USA, Inc.	7:21-cv-07933-VB	United States District Court for the Southern District of New York
Nixon v. Grande Cosmetics, LLC	1:22-cv-06639	United States District Court for the District of New Jersey
Guerrero v. Merritt Healthcare Holdings, LLC	3:23-cv-00389-MPS	United States District Court for the District of Connecticut
Haylee Woodard v. Lilly Lashes, LLC	22STCV18692	Superior Court of California, Los Angeles County
Rave v. Infinity Healthcare Inc.	2019CV003073	Circuit Court for Milwaukee County, Wisconsin
Katz-Lacabe et al v. Oracle America, Inc.	3:22-cv-04792-RS	United States District Court for the Northern District of California
In re Broiler Chicken Antitrust Litigation	16-cv-08637	United States District Court for the Northern District of Illinois
Brooks v. Thomson Reuters Corp.	3:21-cv-01418	United States District Court for the Northern District of California
Hasemann, et al. v. Gerber Products Co., et al.	1:15-cv-02995-EK-RER (E.D.N.Y.)	United States District Court for the Eastern District of New York
Manemeit v. Gerber Products Co.	2:17-cv-00093-EK-RER (E.D.N.Y.)	United States District Court for the Eastern District of New York
Lopez v. Apple, Inc.	4:19-cv-04577-JSW	United States District Court for the Northern District of California
Bush v. Rust-Oleum Corporation, et al.	3:20-cv-03268	United States District Court for the Northern District of California
DeCostanzo v. GlaxoSmithKline PLC, et al	2:2021cv04869	United States District Court for the Eastern District of New York
Mackmin v. Visa Inc.	1:11-cv-01831	United States District Court for the District of Columbia
In re Effexor XR Antitrust Litigation	3:11-cv-05479 (D.N.J.)	United States District Court for the District of New Jersey
Jien et al v. Perdue Farms, Inc. et al	1:2019cv02521	United States District Court for the District of Maryland
Onadia v. City of New York, et al.	300940/2010	Supreme Court of the State of New York, County of Bronx
In re Group Health Plan Litigation	23-cv-00267 (JWB/DJF)	United States District Court for the District of Minnesota



Borozny, et al. v. RTX Corp., Pratt & Whitney Division, et al.	3:21-cv-1657-SVN	United States District Court for the District of Connecticut
Jeffries, et al. v. West Virginia American Water Company	CC-20-2017-C-765	In the Circuit Court of Kanawha County, West Virginia
Pompilio, et al. v. Boar's Head Provisions Co. Inc.	7:24-cv-08220-PMH	United States District Court for the Southern District of New York
Celeste Brown and Ross Finesmith v. AllCare Plus Pharmacy LLC	2484CV02366	Superior Court of Suffolk County, Commonwealth of Massachusetts
Kessler, et al. v. The Quaker Oats Company	7:24-cv-00526-KMK	United States District Court for the Southern District of New York
In Re AT&T Inc. Customer Data Security Breach Litigation MDL	3:24-md-03114-E	United States District Court for the Northern District of Texas
In Re AT&T Inc. Customer Data Security Breach Litigation MDL	3:24-md-03114-E	United States District Court for the Northern District of Texas

21. In each of these cases, ClaimScore was retained to review the claims submitted and, using its proprietary advanced AI analysis (which ClaimScore built specifically to analyze class action claims), provide recommendations to the claims administrator on whether claims were valid or fraudulent. ClaimScore's analyses were adopted by each of the claims administrators and used either in support of final approval or in preparation for payout distribution to the class. Because our service functions as a back-office tool, applied at the discretion of the claim's administrator, its use is typically not referenced in the court's judgement of these cases.

22. The *Nixon v. Grande Cosmetics, LLC* settlement is the one exception. At the initial final approval hearing, the court declined to grant approval due to the unusually high volume of fraudulent claims that persisted, which significantly reduced the expected payout for legitimate class members. Following that hearing, the parties retained ClaimScore, and our analysis was presented at the subsequent final approval hearing. The court granted approval at that stage, due in substantial part to our work. As a result, ClaimScore was specifically referenced in the final judgement in that matter.

23. To reiterate, ClaimScore's analysis was ultimately adopted by the particular claims administrator in each of the above settlements, and in total, ClaimScore's work has resulted in the saving of tens of millions of dollars that otherwise may have been paid to fraudulent actors.

24. Based on our experience in these (and other) cases, it is clear that almost all class

1 action settlements where the identities of all class members are not known (like the present case) are  
2 targets of rampant fraud. Additionally, the sophistication of fraudulently submitted claims we have  
3 seen in these cases makes it clear that that this type of fraud is likely being perpetrated by organized  
4 entities, some of which are international.

5           25. From our review of the claims here, the MarinHealth Settlement has all of the same  
6 hallmarks as the rest, and this case, too, involves a high degree of fraud in the claims process.

7  
8 **A. Technology-based fraud solutions are the standard where money is exchanged**

9           26. Fraud detection has evolved significantly over time. Data-driven methodologies, first  
10 widely adopted in the fintech, financial services, and eCommerce sectors, laid the groundwork for  
11 modern detection strategies by enabling large-scale, real-time analysis of transactional data. These  
12 approaches expanded to incorporate both first-party and third-party data sources, improving the  
13 accuracy of fraud signals by identifying inconsistencies that may not be apparent when viewed in  
14 isolation. As fraud tactics became more sophisticated, detection methods advanced to combine  
15 elements of large-scale data analysis, neural networks, machine learning, and logic-based expert  
16 systems—culminating in hybrid models capable of detecting both well-known fraud vectors and  
17 emerging, complex patterns with precision while maintaining transparency and interpretability.

18  
19           27. ClaimScore’s anti-fraud solution uses this hybrid approach, wherein machine learning  
20 informs the weighting of criteria within our expert system, ensuring adaptability to new fraud  
21 strategies and compliance with evidentiary standards.

22 **B. ClaimScore’s proprietary methodology**

23           28. ClaimScore has developed a unique and proprietary methodology specifically  
24 engineered for use in class actions and mass tort litigation. Our system incorporates real-time pattern  
25 recognition, multi-source data enrichment, and intelligent rule-weighting informed by machine  
26 learning. Since ClaimScore is a software-based solution, its methodology remains consistent across  
27

1 all cases. In other words, the same methodology applied in prior matters is also applied here. The only  
2 exceptions are periodic software updates designed to enhance ClaimScore's fraud detection system.  
3 When such updates are deployed, they are implemented uniformly across both ongoing and future  
4 cases.

5  
6 29. ClaimScore was purpose-built from the ground up to meet the evidentiary and  
7 transparency standards required in federal and state court proceedings. In particular, our use of  
8 machine learning is confined to informing and optimizing our expert system AI – ensuring our  
9 decision-making remains fully auditable, explainable, and compliant with applicable legal  
10 frameworks regarding the use of automated technologies in claim determinations.

11  
12 30. ClaimScore's technology combines a 65+ point expert-system artificial intelligence  
13 algorithm with a neural-network machine learning system to ensure an accurate, objective, and  
14 transparent review of each individual claim made in the settlement of class actions. The platform is  
15 stacked on a complex cloud-architecture that optimizes the speed of the real-time claims analysis.

16  
17 31. Specifically, ClaimScore is provided the 10 or so points of data collected during the  
18 claim submission process (i.e. first name, last name, street address, address 2, city, state, zip, country,  
19 phone number, email, IP address and referrer URL). That data is enriched with over 200 additional  
20 data points using a variety of 1<sup>st</sup> party and 3<sup>rd</sup> party data sources. Those 200 points are distilled down  
21 to the 65+ points that are most useful in distinguishing fraudulent activity from valid submissions.  
22 Our expert system AI traverses those 65+ points, and when indicia of fraud is detected, the claim's  
23 score is reduced, and the claim is tagged with a deduction code. In addition, all case-specific  
24 validation requirements are integrated into ClaimScore's algorithm (i.e. jurisdiction, claimant limit,  
25 household limit, etc.), thus ensuring each claim is accurately evaluated against the requirements set  
26 forth in the settlement agreement.

27  
28 32. Each claim begins with a ClaimScore of 1,000 and as noted above, is reduced each

1 time indicia of fraud is detected. Claims with scores equal to or above 700 are marked as “approved”;  
2 however, if the claim was submitted with a proof of purchase which must be reviewed by a human  
3 prior to final determination and receives a score equal to or greater than 700, ClaimScore marks the  
4 claim as “pending.” Once a claim fails a certain number of criteria, and the ClaimScore drops below  
5 700, ClaimScore recommends that the claim be rejected as non-compliant with the specific terms of  
6 a settlement agreement, including an analysis that the claim contains “indicia of fraud.”

8 33. ClaimScore developed a proprietary neural-network machine learning model to  
9 determine the weight of each step of each criterion based on the prevalence of valid and invalid claims  
10 failing the pertinent criteria step. Once the score weights were established, they were applied to  
11 ClaimScore’s expert system AI algorithm that evaluates each claim against the 65+ points.

12 34. When developing ClaimScore, the score of 700 was selected as the threshold for  
13 rejection, in part because most people are familiar with how the credit score system works, and the  
14 700-metric aligns with that system. A 700-passing score was also selected because a 300-point  
15 deduction would allow claims to fail certain criteria yet still be approved. In other words, potential  
16 claimants are provided with a certain “cushion” to ensure that they are not simply selected for  
17 exclusion based on a single criterion; the claim needs to fail multiple criteria before the score is  
18 reduced to below 700.

19 35. To maximize transparency, each claim is tagged with deduction codes associated with  
20 the criteria it fails, thus ensuring that the parties, the administrator, and the court definitively know  
21 all specific reasons why each claim was rejected. This coding approach creates complete transparency  
22 for each claimant and provides an evidentiary basis for the exclusion of any claims that score below  
23 700.

24 36. To be clear, ClaimScore does not reject claimants based on “one-off” criteria.  
25 ClaimScore refers to this approach as “group and slash.” In contrast, the ClaimScore methodology  
26  
27

1 applies the criteria agreed to in the settlement agreement and measures “other indicia of fraud” against  
2 a full set of criteria to provide each claimant with a score. That score then determines, up front,  
3 whether a claimant actually meets the definition of “class member” pursuant to the settlement  
4 agreement. Under the ClaimScore system, no claim fails simply because it fails to meet a single  
5 criterion.

6  
7 37. An example of a “group and slash” criterion would be the automatic rejection of claims  
8 submitted through a VPN or proxy IP address<sup>1</sup>. By contrast, ClaimScore’s criteria treat the use of a  
9 VPN or proxy as a single deduction, which on its own is not sufficient to reject a claim. Additional  
10 indicia of fraud must be present before a claim would fail under our system. If the “group and slash”  
11 criterion for VPNs had been applied in this case, 532 valid claims (28%) would have been falsely  
12 rejected. Because ClaimScore treated VPN use as a single deduction, those same 532 claims were  
13 ultimately approved by our analysis.

14  
15 38. Other examples of ClaimScore’s criteria include evaluating the validity of an email  
16 address. This is assessed across multiple data points, such as whether the domain’s DNS records are  
17 properly configured to receive email. As with the VPN/proxy example, this factor alone does not  
18 disqualify a claim; however, when combined with other criteria, it may support a “rejected  
19 determination.

20  
21 39. In addition to criteria based on single data points (such as email or IP), ClaimScore  
22 evaluates the overall consistency of data as it relates to the claimant’s identity. Our system identifies  
23 anomalies that are inconsistent with the claimant’s provided identity information. As with the

24  
25  
26 <sup>1</sup> In addition to rejecting claims for use of a VPN or proxy, others outright block access to the claim  
27 form all together if the potential class member is using a VPN or proxy to access the settlement  
28 website. In this instance 28% of valid class members would not have had the opportunity to even file  
a claim.

1 examples above, these anomalies alone are not grounds for rejection, but when combined with other  
2 indicia of fraud, they may result in a claim being marked as “rejected”.

3         40. In order to evaluate accuracy, ClaimScore has conducted several control studies using  
4 tens of thousands of known legitimate claims and the same amount of known invalid claims. In  
5 addition, an independent third party has conducted secondary validations on hundreds of thousands  
6 of claims to evaluate the accuracy of ClaimScore’s analysis. The most recent control study and  
7 independent validation efforts indicated that ClaimScore has an accuracy between 99.987% and  
8 99.996%<sup>2</sup>.

10 **C. ClaimScore’s methodology detects fraud at a much more accurate level**

11         41. As noted, in contrast to the “group and slash” method, ClaimScore utilizes a multi-  
12 factor expert system AI algorithm that evaluates each claim across more than sixty-five (65) distinct  
13 validation points. This difference is critical, and it allows for fraud detection at a much more accurate  
14 level.

15         42. The traditional “group and slash” methodology requires that each selected criterion be  
16 strong enough, on its own, to serve as definitive evidence of fraud. If a claim does not fail that specific  
17 test with absolute clarity, the claim is typically approved – even if, in aggregate, it displays multiple  
18 red flags.

19         43. This single-point approach is ineffective due to the evolution and sophistication of the  
20 fraud schemes being deployed in class action settlements. Fraudsters – some of whom are organized,  
21 international entities – have engineered their submissions, through the use of sophisticated  
22

23 \_\_\_\_\_  
24  
25 <sup>2</sup> The independent third party utilized a multipronged approach to attempt to cure claims identified  
26 by ClaimScore as “rejected”. They used a variety of data sources and also attempted direct  
27 communication with claimants. This resulted in 99.996% of the “rejected” claims being confirmed as  
28 fraudulent. Additionally, ClaimScore’s internal control study, which evaluated known legitimate and  
fraudulent claims, was 99.987% accurate at properly categorizing the claims as either “approved” or  
“rejected”.

1 technology, to circumvent the most commonly used one-off criteria. These bad actors understand  
2 that if they can pass the few limited checks being used, they can gain access to settlement funds,  
3 regardless of whether the rest of their submission lacks credibility.

4         44. In order to properly address this, ClaimScore’s expert system was designed to emulate  
5 the way human experts assess complex data: by considering the totality of circumstances rather than  
6 relying on individual data points in isolation. Under ClaimScore’s methodology, no single failed  
7 criterion is necessarily disqualifying. Instead, each claim begins with a perfect score of 1,000 and is  
8 evaluated against each of the 65+ validation points. Deductions are applied when a claim fails specific  
9 steps within those points. The cumulative effect of these deductions, not any one individual failure,  
10 determines the outcome.

11  
12         45. This approach has a number of critical advantages. First, it allows the system to detect  
13 fraud even when no single piece of evidence would be enough to reject a claim under the traditional  
14 model. Second, because the scoring system is not static and adapts based on real-world data  
15 (including the prevalence of invalid submissions failing specific criteria), it remains highly resistant  
16 to reverse-engineering by fraudsters. In short, while the traditional “one-off” method creates a  
17 checklist that fraudsters can work around – often comprised of no more than twenty-five (25) criteria,  
18 and therefore twenty-five (25) predictable failure points – ClaimScore’s expert system evaluates each  
19 claim against more than sixty-five (65) criteria, resulting in over 35,000,000,000,000,000,000 (35  
20 quintillion) unique scoring combinations. That combinatorial complexity creates a multi-dimensional  
21 validation structure that cannot be bypassed by manipulating any single factor.

22  
23  
24         46. Finally, ClaimScore’s scoring system provides a rigorous, transparent, and evidence-  
25 based framework for rejection. Each deduction is tagged and traceable, ensuring that the exclusion  
26 of a claim is not only statistically valid, but also defensible in legal proceedings. As a result,  
27 ClaimScore is able to recommend rejections not based on speculation, but on a comprehensive and  
28

1 repeatable analysis that has been validated against millions of claims and verified through  
2 independent third-party audits.

3  
4 **V. MarinHealth Settlement Fraud Detection Results**

5 47. Notice was conducted by the Settlement Administrator for the purpose of informing  
6 potential Class Members of the settlement and their rights. The notice plan included Direct Notice  
7 and a Media Campaign. Direct Notice consisted of emailing the summary notice to class members  
8 where email addresses were available and mailing the summary notice by postcard where only  
9 physical addresses were available. If an email notice was returned as undeliverable, the Settlement  
10 Administrator attempted additional email transmissions and, if unsuccessful, mailed a postcard notice  
11 to any available mailing address. For mailed notices returned by the postal services, the settlement  
12 administrator re-mailed to any forwarding address provided and, where appropriate, used address  
13 databases to identify current mailing addresses. In addition, the settlement administrator conducted a  
14 media campaign which included a press release and targeted advertisements place in the North Bay  
15 Business Journal, the Press Democrat, and the Petaluma Argus-Courier.

16  
17 48. ClaimScore was retained to evaluate the claims for fraud to ensure that the net  
18 settlement fund is distributed only to valid Class Members.

19  
20 49. Verita facilitated the secure transfer of claim submission data for the initial 62,423  
21 claims to ClaimScore via one CSV file. Prior to review, ClaimScore was also provided with the  
22 Settlement Agreement and other publicly available documents from the settlement website  
23 (<https://www.marinhealthsettlement.com/>).

24  
25 50. Thereafter, the claims were analyzed using ClaimScore's retroactive claim review  
26 platform. Following this review, ClaimScore conducted a Quality Assurance (QA) audit to assess  
27 whether any new fraud vectors had emerged since the most recent system update. The results of that



1 QA process confirmed that the latest version of ClaimScore remains effective in detecting the most  
2 advanced forms of class action claim fraud.

3 51. According to ClaimScore's analysis, of the 62,423 claims transferred to ClaimScore,  
4 1,894 claims scored 700 or above and were recommended as "Approved", 60,528 claims scored  
5 below 700 and were recommended for "Rejection".  
6

7 52. Of the 60,528 claims that scored below 700, 75.71% had at least three (3) indicators  
8 of fraud.

9 53. As noted above, updated results will be provided following the conclusion of the  
10 Claims Period and upon completion of our final analysis.  
11

12  
13 I declare under penalty of perjury under the laws of the United States of America that the foregoing  
14 is true and correct.

15 DATED: September 8, 2025

16  
17 By:   
18 Bryan Heller  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28