UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

OMER CYGLER, Individually and on behalf of all others similarly situated, Plaintiff, v. ALARUM TECHNOLOGIES LTD., SHACHAR DANIEL, and SHAI AVNIT, Defendants.	**Case No:** **CLASS ACTION COMPLAINT FOR VIOLATIONS OF THE FEDERAL SECURITIES LAWS** **JURY TRIAL DEMANDED**

Plaintiff Omer Cygler ("Plaintiff"), individually and on behalf of all other persons similarly situated, by Plaintiff's undersigned attorneys, for Plaintiff's complaint against Defendants (defined below), alleges the following based upon personal knowledge as to Plaintiff and Plaintiff's own acts, and information and belief as to all other matters, based upon, among other things, the investigation conducted by and through his attorneys, which included, among other things, a

review of the Defendants' public documents, public filings, wire and press releases published by and regarding Alarum Technologies Ltd. ("Alarum", "Alarum Technologies," or the "Company"), and information readily obtainable on the Internet. Plaintiff believes that substantial evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery. [1]

NATURE OF THE ACTION

1. This is a class action on behalf of persons or entities who purchased or otherwise acquired publicly traded Alarum securities between March 20, 2025 and July 2, 2026, inclusive (the "Class Period"). Plaintiff seeks to recover compensable damages caused by Defendants' violations of the federal securities laws under the Securities Exchange Act of 1934 (the "Exchange Act").

JURISDICTION AND VENUE

2. The claims asserted herein arise under and pursuant to Sections 10(b) and 20(a) of the Exchange Act (15 U.S.C. §§ 78j(b) and 78t(a)) and Rule 10b-5 promulgated thereunder by the SEC (17 C.F.R. § 240.10b-5).

[1] Unless otherwise stated, all emphasis is added and internal citations are omitted

3. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331, and Section 27 of the Exchange Act (15 U.S.C. §78aa).

4. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) and Section 27 of the Exchange Act (15 U.S.C. § 78aa(c)) as the alleged misstatements entered and the subsequent damages took place in this judicial district.

5. In connection with the acts, conduct and other wrongs alleged in this complaint, Defendants (defined below), directly or indirectly, used the means and instrumentalities of interstate commerce, including but not limited to, the United States mails, interstate telephone communications and the facilities of the national securities exchange.

PARTIES

6. Plaintiff, as set forth in the accompanying certification, incorporated by reference herein, purchased Alarum securities during the Class Period and was economically damaged thereby.

7. Defendant Alarum has stated the following about its business:

> We are a global provider of web data collection solutions, empowering organizations to gain a competitive edge by streamlining the collection, extraction, and analysis of large-scale structured data from public online sources.

8. Defendant Alarum is incorporated under the laws of the State of Israel and its principal executive offices are located at 8 Yitzhak Sade Street, Tel Aviv, 6777508. It does not maintain offices in the United States.

9. Alarum's American Depositary Shares ("ADS" or "ADSs") trade on the Nasdaq Capital Market ("NASDAQ") under the ticker symbol "ALAR".

10. Defendant Shachar Daniel ("Daniel") served as Alarum's Chief Executive Officer ("CEO") at all relevant times.

11. Defendant Shai Avnit ("Avnit") served as Alarum's Chief Financial Officer ("CFO") at all relevant times.

12. Defendants Daniel and Avnit are collectively referred to herein as the "Individual Defendants."

13. Each of the Individual Defendants:

(a) directly participated in the management of the Company;

(b) was directly involved in the day-to-day operations of the Company at the highest levels;

(c) was privy to confidential proprietary information concerning the Company and its business and operations;

(d) was directly or indirectly involved in drafting, producing, reviewing and/or disseminating the false and misleading statements and information alleged herein;

(e) was directly or indirectly involved in the oversight or implementation of the Company's internal controls;

(f) was aware of or recklessly disregarded the fact that the false and misleading statements were being issued concerning the Company; and/or

(g) approved or ratified these statements in violation of the federal securities laws.

14. Alarum is liable for the acts of the Individual Defendants and its employees under the doctrine of *respondeat superior* and common law principles of agency because all of the wrongful acts complained of herein were carried out within the scope of their employment.

15. The scienter of the Individual Defendants and other employees and agents of the Company is similarly imputed to Alarum under *respondeat superior* and agency principles.

16. Defendant Alarum and the Individual Defendants are collectively referred to herein as "Defendants."

SUBSTANTIVE ALLEGATIONS

Materially False and Misleading Statements Issued During the Class Period

17. On March 20, 2025, before market open, the Company filed with the SEC its Annual Report on Form 10-K for the year ended December 31, 2024 (the

"2024 Annual Report"). Attached to the 2024 Annual Report were signed certifications pursuant to the Sarbanes-Oxley Act of 2002 ("SOX") signed by Defendants Daniel and Avnit attesting to the accuracy of financial reporting, the disclosure of any material changes to the Company's internal controls over financial reporting, and the disclosure of all fraud.

18. The 2024 Annual Report contained the following statement regarding a subsidiary called NetNut Ltd. (which also has a Delaware subsidiary, collectively "NetNut") and Alarum's purported "main advantages over competitors", which included in part:

- NetNut's web data collection service has been designed to handle massive amounts of traffic, with the capacity to process hundreds of terabytes per second, while ensuring the data collection process is not blocked.
- NetNut has formed strategic partnerships with leading ISPs and technology providers to enhance its network capabilities and offer customers the best possible solution.
- NetNut's solution has been rigorously tested and validated by independent research firms and experts in the field.
- NetNut's solution has received positive feedback from customers, with many praising its fast, secure, and reliable performance.

19. The statement in ¶ 18 was materially false and misleading at the time it was made because it extolled purported NetNut advantages while omitting that NetNut engaged in unlawful behavior that materially raised Alarum's risk profile and called into question its business prospects.

20. The 2024 Annual Report contained the following statement about NetNut:

> Our web data collection solutions are provided through our wholly owned subsidiary ***NetNut and offer secured, fast, and anonymous IPPN Solutions to our business customers which, in turn, enables them to anonymously and securely browse the internet as well as to collect data from any publicly available source on the web, for their own business purposes***. Our IPPN solutions allow organizations to collect vast amounts of accurate, transparent web data from public online sources by simultaneously connecting to the Internet from different IP addresses. Our customers can choose from various types of IPs from our IP pool which contains millions of IPs, including ISP IPs, data center IPs, and residential service provider IPs.

21. The statement in ¶ 20 was materially false and misleading at the time it was made for the same reasons outlined in ¶ 19.

22. The 2024 Annual Report contained the following risk disclosure:

> ***Our reputation and business could be harmed based on real or perceived shortcomings, defects or vulnerabilities in our solution or the failure of our solution to meet customers' expectations.*** **[Emphasis in original].**
> Organizations and consumers are facing increasingly sophisticated and targeted cyber threats, including the growing threat of cyber terrorism throughout the world. ***If we fail to identify and respond to new and increasingly complex methods of attack and update our products to detect or prevent such threats, our business and reputation will suffer***. In particular, we may suffer significant adverse publicity and reputational harm if a significant breach occurs generally or if any breach occurs at a high-profile customer. Moreover, if our solutions are adopted by an increasing number of enterprises and consumers, it is possible that attackers will begin to focus on finding ways to defeat our solutions. ***An actual or perceived security breach or theft of our customers' sensitive business or personal data, regardless of whether the breach or theft is attributable to the failure of our products, could adversely affect the market's perception of the efficacy of our solutions and current or potential customers may look to our competitors for alternatives to our solutions***. The failure of our products may also subject us to lawsuits and financial losses stemming from

> indemnification demands of our partners and other third parties, as well as the expenditure of significant financial resources to analyze, correct or eliminate any vulnerabilities. Any claim brought against us, regardless of its merit, could result in material expense, diversion of management time and attention, and damage to our reputation, and could cause us to fail to retain or attract customers. Costs or payments made in connection with warranty and product liability claims and product recalls, or other claims could materially affect our financial condition and results of operations. It could also cause us to suffer reputational harm, lose existing customers or deter them from purchasing additional products and services and prevent new customers from purchasing our solutions.
>
> False detection of threats, while typical in our industry, may reduce perception of the reliability of our products and may therefore adversely impact market acceptance of our products. If our solutions restrict legitimate privileged access by authorized personnel to IT systems and applications by falsely identifying those users as an attack or otherwise unauthorized, or fail to provide privacy and security web browsing to consumers, our customers' businesses could be harmed. There can be no assurance that, despite testing by us, errors will not be found in existing and new versions of our products, resulting in loss of or delay in market acceptance. In such an event, we may be required, or may choose, for customer relations or other reasons, to expend additional resources in order to help correct the problem. In addition, the network of data collection solutions is built on a mix of IPs, which we source from various providers and technologies. A significant portion of our IP pool is sourced from third-party IP proxy providers and ISPs around the world from which we lease and then resell. We have separate agreements with each provider. If such a provider chooses to terminate the agreement, we will be at a risk of reducing the size of our IP pool and might not be able to support the demands of our customer base.

23. The statements in ¶ 22 was materially false at the time it was made because it omitted that NetNut engaged in illegal activity by linking customer home internet devices into another network that others, including cyber criminals, could surreptitiously join in order to remain anonymous, and create the appearance that the wrongdoing was committed by an innocent Alarum customer. In so doing,

Alarum *enabled* cyber criminals at the expense of its own customers and in so doing, materially threatened its own business prospects and materially raised the risk of material reputational damage and legal exposure.

24. The 2024 Annual Report contained the following risk disclosure:

> ***If we are unable to acquire new customers, our future revenues and operating results will be harmed.*** **[Emphasis in original]**
>
> Our success depends on our ability to acquire new customers. The number of customers that we add in a given period impacts both our short-term and long-term revenues. ***If we are unable to attract a sufficient number of new customers, we may be unable to generate revenue growth at desired rates. The markets we operate in are competitive and many of our competitors have substantial financial, personnel, and other resources that they utilize to develop products and attract customers***. As a result, it may be difficult for us to add new customers to our customer base. Competition in the marketplace may also lead us to win fewer new customers or result in us providing discounts and other commercial incentives. Additional factors that impact our ability to acquire new customers include the perceived need for cyber security, the size of our prospective customers' infrastructure budgets, the utility and efficacy of our existing and new offerings, whether proven or perceived, our ability to reach a significant portion of the consumer market, and general economic conditions. These factors may have a meaningful negative impact on future revenues and operating results. With respect to our enterprise access business, while many companies understand the problem of doing competitive analysis, data collection, and other privacy-related use cases, widespread awareness of the need for access solutions is still lacking. Proxy networks are well understood, and virtual private networks are commonly popular, but access solutions are still in the early adoption phase among companies and individuals that stand to benefit from them. This restraint accounts for not all enterprise access vendors having the marketing budgets to promote themselves.

25. The statement in ¶ 24 was materially false and misleading at the time it was made because it materially understated the risk of the Company being unable

to acquire new customers, given that NetNut was engaging in illegal activity that materially threatened Alarum's business prospects.

26. The 2024 Annual Report contained the following risk disclosure, which stated in part:

> ***If our internal network system is compromise[d] by cyber attackers or other malicious cyber activity, or if our hosting and infrastructure fails, public perception of our products and services will be harmed.*** **[Emphasis in original].**
>
> We will not succeed unless the marketplace is confident that we provide effective cybersecurity protection. Further, we may be targeted by cyber terrorists because we are an Israeli company or otherwise. For example, in January 2023, we experienced an immaterial breach, which resulted in the hacker gaining temporary access to our database. In response, we secured all exposed servers to prevent further breaches and engaged a Chief Information Security Officer (CISO) to provide security consultation and strengthen our defenses. Although such incident did not have an adverse effect on us or our customers and we have not had a cybersecurity incident since then, if we experience another actual or perceived breach of our network and our internal systems, it could adversely affect the market perception of our products and services. In addition, we may need to devote more resources to address security vulnerabilities in our solution, and the cost of addressing these vulnerabilities could reduce our operating margins. ***If we do not address security vulnerabilities or otherwise provide adequate security features in our products, certain customers, particularly government customers, may delay or stop purchasing our products. Further, a security breach could impair our ability to operate our business, including our ability to provide maintenance and support services to our customers***. If this happens, our revenues could decline, and our business could suffer. If we experience short period hosting/infrastructure failures, or longer periods of disconnection blocking of our network of IPs to access certain websites, and do not offer our customers various immediate alternatives, some customers may choose to delay or stop purchasing our products.
>
> * * *

> Information technology systems, including those managed or hosted by third parties, could be subject to sophisticated cyber-attacks (including phishing and ransomware attacks) and threats by external or internal parties' intent on disrupting business processes or otherwise extracting or corrupting information. In recent years, ransomware attacks against organizations have become more frequent and while we continue to implement additional protective measures to reduce the risk of and detect cyber incidents, cyber-attacks are becoming more sophisticated and frequent, and the techniques used in such attacks change rapidly. We may also face increased cybersecurity risks due to the number of our employees and our third-party providers' who are (and may continue to be) working remotely, which creates additional opportunities for cybercriminals to launch attacks and exploit vulnerabilities in non-corporate IT environments. Unauthorized access to our systems could disrupt our business, and/or lead to theft, loss or misappropriation of critical assets or to outside parties having access to confidential information, including privileged data, personal data or strategic information. Such information could also be made public in a manner that harms our reputation and financial results and, particularly in the case of personal data, could lead to regulators imposing significant fines on us.

27. The statement in ¶ 26 was materially false and misleading at the time it was made because it omitted that NetNut engaged in illegal activity that had the effect of helping cyber criminals (by virtue of using networks owned by Alarum customers anonymously), which could foreseeably create legal exposure for unwitting Alarum customers.

28. The 2024 Annual Report contained the following risk disclosure:

> ***If our products fail to ensure customer compliance with government regulations and industry standards, our business and results could be materially impacted.*** **[Emphasis in original].**
>
> The legality of scraping publicly available web data was first upheld in late 2019, when the Ninth Circuit Court of Appeals ruled in hiQ Labs, Inc. v. LinkedIn Corporation that scraping publicly accessible data did not violate the Computer Fraud and Abuse Act. This decision, which favored hiQ Labs,

Inc. over LinkedIn Corporation, reinforced the legality of accessing publicly available online data, despite LinkedIn Inc.'s objections. The Ninth Circuit reaffirmed this ruling in April 2022, setting a critical precedent for data collection practices involving publicly accessible information. However, as the web continues to evolve as a vast source of information, the debate over data accessibility versus privacy is likely to intensify, as well as in connection with the way in which some of the automated software programs are built, and changes in regulations may impact the means or ability to provide such solutions. For instance, X Corp. (formerly Twitter) has filed several lawsuits against parties accused of scraping its platform without consent. Additionally, Meta Platforms, Inc. v. Bright Data Ltd. is another significant case that could influence legal perspectives on this issue. In this case, Meta Platforms, Inc. argues that scraping its publicly available data violates user agreements and intellectual property protections. As the web evolves as a vast source of information, the debate over data accessibility versus privacy will likely intensify. This includes concerns over how automated software programs are built, as well as the potential for changes in regulations that could affect the ability to provide such solutions.

International regulatory bodies are increasingly focused on online privacy issues and user data protection. In particular, the General Data Protection Regulation, or the GDPR, in the European Union, or EU, and the UK intends to strengthen and unify data protection for all individuals within the EU. It also addresses the export of personal data outside the EU. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. Additionally, the uncertainty created by these laws and regulations can be compounded when services hosted in one jurisdiction are directed at users in another jurisdiction. For instance, European data protection rules may apply to companies which are not established in the EU (this is the so-called extraterritorial scope of the GDPR). Similarly, there have been laws and regulations adopted throughout the United States and Israel that impose obligations in areas such as privacy, in particular protection of personal information and implementing adequate cybersecurity measures to protect such information. The most prominent to which we are exposed is the California Consumer Privacy Act of 2020, or the CCPA, which increases the privacy and security obligations companies have towards the consumer when handling personal data. The CCPA allows civil penalties for violations as well as private right of action for data breaches. In addition, the California Privacy Rights Act, or the CPRA, which became

> effective as of January 1, 2023, imposes additional obligations such as expanding the current data privacy compliance requirements under the CCPA. As an Israeli company we are also subject to the Israeli Privacy Protection Law 1981 and its regulations, as well as the guidelines of the Israeli Privacy Protection Authority.
>
> These industry standards may change with little or no notice, including changes that could make them more or less onerous for businesses. Any inability to adequately address privacy and security concerns or comply with applicable privacy and data security laws, rules and regulations could have an adverse effect on our business prospects, results of operations and/or financial position. In addition, governments may also adopt new laws or regulations, or make changes to existing laws or regulations, that could impact whether our solution enables our customers to maintain compliance with such laws or regulations. If we are unable to adapt our solution to changing government regulations and industry standards in a timely manner, or if our solution fails to expedite our customers' compliance initiatives, our customers may lose confidence in our products and could switch to products offered by our competitors. In addition, if government regulations and industry standards related to the access sectors are changed in a manner that makes them less onerous, our customers may view compliance as less critical to their businesses, and our customers may be less willing to purchase our products and services. In either case, our sales and financial results would suffer.

29. The statement in ¶ 28 was materially false and misleading at the time it was made because it discussed legal compliance while omitting that NetNut was actively engaging in illegal activity.

30. On March 19, 2026 the Company filed with the SEC its Annual Report on Form 10-K for the year ended December 31, 2025 (the "2025 Annual Report"). Attached to the 2024 Annual Report were signed certifications pursuant to SOX signed by Defendants Daniel and Avnit attesting to the accuracy of financial

reporting, the disclosure of any material changes to the Company's internal controls over financial reporting, and the disclosure of all fraud.

31. The 2025 Annual Report contained substantially similar statements as the ones contained in ¶¶ 18, 22, 24, 26 and 28.

32. As a result, those statements were materially false and misleading at the time they were made for the reasons stated in ¶¶ 19, 23, 25, 27 and 29

33. The statements contained in ¶¶ 18, 20, 22, 24, 26, and 28 were materially false and/or misleading because they misrepresented and failed to disclose the following adverse facts pertaining to the Company's business, operations and prospects, which were known to Defendants or recklessly disregarded by them. Specifically, Defendants made false and/or misleading statements and/or failed to disclose that: (1) an Alarum Technologies subsidiary, NetNut, was engaging in illegal activity by linking customer home internet devices into another network without the customer's consent; (2) this activity allows cyber criminals to conceal their locations; (3) the foregoing materially heightened Alarum Technologies' legal exposure and materially threatened its business prospects; and (4) as a result, Defendants' statements about Alarum Technologies' business, operations, and prospects were materially false and misleading and/or lacked a reasonable basis at all relevant times.

THE TRUTH BEGINS TO EMERGE

34. On July 2, 2026, during market hours, *Reuters* published an article entitled "Google disrupts NetNut proxy network used in malware operations." The article stated the following:

> Google said on Thursday it weakened a network of internet-connected devices being used to conceal and route malicious online traffic, ***acting against the NetNut residential proxy operator and the Popa botnet.***
>
> ***Google took action in partnership with the FBI and [Lumen], among others***.
>
> The tech giant said it disabled accounts and services used in NetNut-related malware command-and-control operations and shared technical intelligence on the group's infrastructure with law enforcement and industry partners to support broader enforcement efforts.
>
> ***Residential proxy networks route internet traffic through consumer IP addresses, masking its origin and bypassing security defenses, a feature that, while having legitimate uses, is frequently exploited for cybercrime***. "***We believe our coordinated actions have caused significant degradation to NetNut's proxy network and its business operations, reducing the available pool of devices for the proxy operator by millions***," Google said in a blog.

35. On this news, Alarum ADSs fell $1.67 per share, or 20.8%, to close at $6.35 per ADS on July 2, 2026.

36. On July 2, 2026, after market hours, Alarum issued a press release entitled "Alarum Technologies Responds to Inquiry into Residential Proxy Networks." The press release stated, in pertinent part, the following:

> On July 2, 2026, Alarum and its subsidiary NetNut Ltd. ("NetNut") were made aware of the seizure of certain domains associated with NetNut by the FBI. ***Alarum takes this matter seriously and will fully cooperate with law enforcement to ensure any misuse of its infrastructure is thoroughly investigated and those responsible are held to account***.

37. Also on July 2, 2026, after market hours, Bloomberg published an article entitled "FBI Probes Whether Alarum Unit is Behind Co-Opted Home Devices." The article stated the following:

> The FBI is investigating whether a subsidiary of the data-collection firm [Alarum] ***had a role in linking customers' home internet devices without their consent into a network that people can use to disguise their locations***, according to documents seen by Bloomberg News and confirmed by people familiar with the situation.
>
> The investigation involves what are known as residential proxy networks that are capable of routing internet traffic for users in a way that appears as if it's coming from a different location. Businesses routinely use these networks to customize their websites for different regions. Sports fans might also take advantage of them to stream games only available for viewing in other places.
>
> ***For more than a year***, [FBI] agents have been examining potential links between NetNut, the Israel-based Alarum subsidiary that sells access to such networks, and software known as Popa that's allegedly used to co-opt people's devices, ***according to records and people familiar with the matter who asked not to be identified discussing an active investigation***.
>
> The Department of Justice said Thursday that the FBI seized multiple internet domains as part of a "coordinated law enforcement targeting infrastructure associated with NetNut's residential proxy platforms, its administrators and its users."
>
> * * *
>
> These networks run off specialized code installed on everyday devices such as laptops, smartphones, routers and TV streaming boxes. Sometimes device owners agree to install the software in exchange for a few dollars a month. In other instances, devices are enrolled into residential proxy networks without their owners' knowledge, according to cybersecurity efforts.

38. The article quoted Craig Labovitz, head of technology for Nokia Deepfield, a network security platform, as stating that "***I think of residential proxy***

like thousands of anonymous strangers sneaking into your home to get unlimited internet access." Further, "[m]ost users may ***not even notice the uninvited proxy internet squatters until the police come to their door investigating cybercrime coming from the home***."

39. The article further stated that the FBI's investigation, which it noted had not been previously reported, is "part of a broader law enforcement effort to scrutinize the uses of residential proxy networks."

40. Then, on July 3, 2026 (which was not a trading day in the United States), Alarum issued a press release entitled "Alarum Technologies Provides Update Regarding Recent Law Enforcement Action." The release stated, in pertinent part, the following:

> [Alarum] today provided a further update to its announcement issued on July 2, 2026 regarding recent reports concerning its proxy network operations.
>
> As previously disclosed, on July 2, 2026, the Company and its subsidiary, NetNut Ltd. ("NetNut"), became aware that certain domains associated with NetNut had been seized by the U.S. Federal Bureau of Investigations ("FBI").
>
> ***Since that announcement, the Company has continued to analyze the incident and additional domains associated with NetNut have also been seized***.
>
> ***As a result of these developments, the Company is currently experiencing disruptions to a portion of its services. If these disruptions continue for an extended period, they are likely to have a material adverse effect on the Company's operations, financial results and its ability to provide certain services to its customers***.
>
> The Company is devoting substantial resources to investigating the

circumstances surrounding these events and is working intensively to obtain additional information regarding the nature and scope of the incident. As of the date and time of this press release, neither the Company nor NetNut has been formally contacted by the FBI or any other governmental or regulatory authority in connection with these matters.

The Company itself is continuing to investigate whether its network or services have been used for malicious, fraudulent or unlawful purposes by third parties. Alarum takes this matter seriously and will fully cooperate with law enforcement to ensure any misuse of its infrastructure is thoroughly investigated and those responsible are held to account.

41. Then, on July 4, 2026, Alarum issued a press release entitled "Alarum Technologies Announces Temporary Operational Pause of Certain Network Services," which stated in pertinent part the following:

Further to [Alarum's] announcements dated July 2 and July 3, 2026, the Company continues to investigate the recent incident affecting certain aspects of NetNut Ltd's network.

As part of this ongoing investigation, and as a precautionary operational measure, the Company has decided to temporarily pause traffic through the relevant network services for several days. This step is intended to enable the Company to investigate the incident, assess the affected infrastructure, determine whether any malicious activity occurred, and implement any measures the Company determines are appropriate before resuming normal operations.

The Company believes that temporarily pausing traffic through the relevant network services is the most responsible course of action while the investigation is ongoing.

As a result of this temporary operational measure, the availability of the Company's services will be significantly reduced during this period. The Company has taken this precautionary step to enable a thorough investigation of the incident and is devoting substantial technical and operational resources to the investigation and recovery process. The Company is working to restore normal operations as soon as possible.

The Company continues to evaluate the situation and will provide additional updates as appropriate.

42. On this news, the price of Alarum ADSs fell $3.27 per share, or 51.49%, to close at $3.08 per share on July 6, 2026.

43. As of the date of the filing of this complaint, Alarum's investor related website has been seized by the FBI, as illustrated below:

44. As a result of Defendants' wrongful acts and omissions, and the precipitous decline in the market value of the Company's common shares, Plaintiff and other Class members have suffered significant losses and damages.

PLAINTIFF'S CLASS ACTION ALLEGATIONS

45. Plaintiff brings this action as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3) on behalf of a class consisting of all persons other

than defendants who acquired Alarum securities publicly traded on the NASDAQ during the Class Period, and who were damaged thereby (the "Class"). Excluded from the Class are Defendants, the officers and directors of Alarum, members of the Individual Defendants' immediate families and their legal representatives, heirs, successors or assigns and any entity in which Defendants have or had a controlling interest.

46. The members of the Class are so numerous that joinder of all members is impracticable. Throughout the Class Period, Alarum securities were actively traded on NASDAQ. While the exact number of Class members is unknown to Plaintiff at this time and can be ascertained only through appropriate discovery, Plaintiff believes that there are hundreds, if not thousands of members in the proposed Class.

47. Plaintiff's claims are typical of the claims of the members of the Class as all members of the Class are similarly affected by defendants' wrongful conduct in violation of federal law that is complained of herein.

48. Plaintiff will fairly and adequately protect the interests of the members of the Class and has retained counsel competent and experienced in class and securities litigation. Plaintiff has no interests antagonistic to or in conflict with those of the Class.

49. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual members of the Class. Among the questions of law and fact common to the Class are:

- whether the Exchange Act was violated by Defendants' acts as alleged herein;
- whether statements made by Defendants to the investing public during the Class Period misrepresented material facts about the business and financial condition of Alarum;
- whether Defendants' public statements to the investing public during the Class Period omitted material facts necessary to make the statements made, in light of the circumstances under which they were made, not misleading;
- whether the Defendants caused Alarum to issue false and misleading filings during the Class Period;
- whether Defendants acted knowingly or recklessly in issuing false filings;
- whether the prices of Alarum securities during the Class Period were artificially inflated because of the Defendants' conduct complained of herein; and

- whether the members of the Class have sustained damages and, if so, what is the proper measure of damages.

50. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in the management of this action as a class action.

51. Plaintiff will rely, in part, upon the presumption of reliance established by the fraud-on-the-market doctrine in that:

- Alarum shares met the requirements for listing, and were listed and actively traded on NASDAQ, an efficient market;
- As a public issuer, Alarum filed periodic public reports;
- Alarum regularly communicated with public investors via established market communication mechanisms, including through the regular dissemination of press releases via major newswire services and through other wide-ranging public disclosures, such as communications with the financial press and other similar reporting services;

- Alarum' securities were liquid and traded with moderate to heavy volume during the Class Period; and
- Alarum was followed by a number of securities analysts employed by major brokerage firms who wrote reports that were widely distributed and publicly available.

52. Based on the foregoing, the market for Alarum securities promptly digested current information regarding Alarum from all publicly available sources and reflected such information in the prices of the shares, and Plaintiff and the members of the Class are entitled to a presumption of reliance upon the integrity of the market.

53. Alternatively, Plaintiff and the members of the Class are entitled to the presumption of reliance established by the Supreme Court in *Affiliated Ute Citizens of the State of Utah v. United States*, 406 U.S. 128 (1972), as Defendants omitted material information in their Class Period statements in violation of a duty to disclose such information as detailed above.

COUNT I
For Violations of Section 10(b) And Rule 10b-5 Promulgated Thereunder Against All Defendants

54. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

55. This Count is asserted against Defendants is based upon Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), and Rule 10b-5 promulgated thereunder by the SEC.

56. During the Class Period, Defendants, individually and in concert, directly or indirectly, disseminated or approved the false statements specified above, which they knew or deliberately disregarded were misleading in that they contained misrepresentations and failed to disclose material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading.

57. Defendants violated §10(b) of the 1934 Act and Rule 10b-5 in that they:

- employed devices, schemes and artifices to defraud;
- made untrue statements of material facts or omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; or
- engaged in acts, practices and a course of business that operated as a fraud or deceit upon plaintiff and others similarly situated in connection with their purchases of Alarum securities during the Class Period.

58. Defendants acted with scienter in that they knew (or otherwise were deliberately reckless in not knowing) that the public documents and statements issued or disseminated in the name of Alarum were materially false and misleading as a result of the fact that NetNut engaged in illegal behavior; knew that such statements or documents would be issued or disseminated to the investing public; and knowingly and substantially participated, or acquiesced in the issuance or dissemination of such statements or documents as primary violations of the securities laws. These defendants by virtue of their receipt of information reflecting the true facts of Alarum, their control over, and/or receipt and/or modification of Alarum' allegedly materially misleading statements, and/or their associations with the Company which made them privy to confidential proprietary information concerning Alarum, participated in the fraudulent scheme alleged herein. To date, Alarum has provided no competing inference to the allegation that NetNut engaged in illegal activity.

59. Individual Defendants, who are the senior officers and/or directors of the Company, had actual knowledge of the material omissions and/or the falsity of the material statements set forth above, and intended to deceive Plaintiff and the other members of the Class, or, in the alternative, acted with reckless disregard for the truth when they failed to ascertain and disclose the true facts in the statements

made by them or other Alarum personnel to members of the investing public, including Plaintiff and the Class.

60. As a result of the foregoing, the market price of Alarum securities was artificially inflated during the Class Period. In ignorance of the falsity of Defendants' statements, Plaintiff and the other members of the Class relied on the statements described above and/or the integrity of the market price of Alarum securities during the Class Period in purchasing Alarum securities at prices that were artificially inflated as a result of Defendants' false and misleading statements.

61. Had Plaintiff and the other members of the Class been aware that the market price of Alarum securities had been artificially and falsely inflated by Defendants' misleading statements and by the material adverse information which Defendants did not disclose, they would not have purchased Alarum securities at the artificially inflated prices that they did, or at all.

62. As a result of the wrongful conduct alleged herein, Plaintiff and other members of the Class have suffered damages in an amount to be established at trial.

63. By reason of the foregoing, Defendants have violated Section 10(b) of the 1934 Act and Rule 10b-5 promulgated thereunder and are liable to the plaintiff and the other members of the Class for substantial damages which they suffered in connection with their purchase of Alarum securities during the Class Period.

COUNT II
Violations of Section 20(a) of the Exchange Act
Against the Individual Defendants

64. Plaintiff repeats and realleges each and every allegation contained in the foregoing paragraphs as if fully set forth herein.

65. During the Class Period, the Individual Defendants participated in the operation and management of Alarum, and conducted and participated, directly and indirectly, in the conduct of Alarum' business affairs. Because of their senior positions, they knew the adverse non-public information about Alarum's business practices.

66. As officers and/or directors of a publicly owned company, the Individual Defendants had a duty to disseminate accurate and truthful information with respect to Alarum' financial condition and results of operations, and to correct promptly any public statements issued by Alarum which had become materially false or misleading.

67. Because of their positions of control and authority as senior officers, the Individual Defendants were able to, and did, control the contents of the various reports, press releases and public filings which Alarum disseminated in the marketplace during the Class Period concerning Alarum' results of operations. Throughout the Class Period, the Individual Defendants exercised their power and authority to cause Alarum to engage in the wrongful acts complained of herein. The

Individual Defendants therefore, were "controlling persons" of Alarum within the meaning of Section 20(a) of the Exchange Act. In this capacity, they participated in the unlawful conduct alleged which artificially inflated the market price of Alarum securities.

68. By reason of the above conduct, the Individual Defendants are liable pursuant to Section 20(a) of the Exchange Act for the violations committed by Alarum.

PRAYER FOR RELIEF

WHEREFORE, plaintiff, on behalf of himself and the Class, prays for judgment and relief as follows:

(a) declaring this action to be a proper class action, designating plaintiff as Lead Plaintiff and certifying plaintiff as a class representative under Rule 23 of the Federal Rules of Civil Procedure and designating plaintiff's counsel as Lead Counsel;

(b) awarding damages in favor of plaintiff and the other Class members against all defendants, jointly and severally, together with interest thereon;

awarding plaintiff and the Class reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

(d) awarding plaintiff and other members of the Class such other and further relief as the Court may deem just and proper.