UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

_____, 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** **DEMAND FOR JURY TRIAL**

Plaintiff _____ ("Plaintiff"), individually and on behalf of all others similarly situated, by and through his attorneys, alleges the following upon information and belief, except as to those allegations concerning Plaintiff, which are alleged upon personal knowledge. Plaintiff's information and belief is based upon, among other things, his counsel's investigation, which includes without limitation: (a) review and analysis of regulatory filings made by Alarum Technologies Ltd. ("Alarum" or the "Company") with the United States ("U.S.") Securities and Exchange Commission ("SEC"); (b) review and analysis of press releases and media reports issued by and disseminated by Alarum; and (c) review of other publicly available information concerning Alarum.

NATURE OF THE ACTION AND OVERVIEW

1. This is a class action on behalf of persons and entities that purchased or otherwise acquired Alarum securities between March 29, 2022 and July 2, 2026, inclusive (the "Class Period"). Plaintiff pursues claims against the Defendants under the Securities Exchange Act of 1934 (the "Exchange Act").

2. Alarum[1] provides web data collection and proxy services. As of December 31, 2025, the Company has one operating and reportable segment: the Web Data Collection segment. This segment is powered by its subsidiary, NetNut Ltd. ("NetNut"). Alarum acquired NetNut in 2019. Alarum heavily invested in its infrastructure, and by mid-2023, Alarum shifted its main focus strictly to NetNut's operations. NetNut purports to provide tools to gather, extract, and analyze large-scale structured data from public online sources.

3. On June 18, 2026, after the market closed, popular cybersecurity blog Krebs on Security reported that several security firms allegedly linked NetNut with a pervasive botnet

[1] Formerly known as Safe-T Group Ltd.

named Popa. The report stated[2] "***for the past four years,***" "Popa has forced millions of consumer TV boxes to relay Internet traffic linked to advertising fraud, account takeovers, and mass data-scraping efforts." "This week, researchers from multiple security firms concluded that the ***Popa botnet is linked to NetNut, . . . operated by the publicly-traded Israeli firm Alarum Technologies Ltd***."

4. On this news, the Company's share price fell $0.76 or 8.3%, to close at $8.41 on June 22, 2026, on unusually heavy trading volume.

5. On July 2, 2026, at approximately 2:00 PM EST, REUTERS reported Google had taken action against 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 reportedly "***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." The article stated "NetNut's parent, Israel-based web data provider Alarum Technologies was informed of the ***seizure of some of its domains by the FBI on Thursday***, the company told Reuters."

6. On this news, the Company's share price fell $1.67 or 20.81%, to close at $6.35 on July 2, 2026, on unusually heavy trading volume.

7. On July 2, 2026, after the market closed, BLOOMBERG NEWS revealed details of the FBI's investigation into ***NetNut on claims it may have a "role in linking customers' home internet devices without their consent into a network that people can use to disguise their locations"*** via a "software known as Popa that's allegedly used to co-opt people's devices."

[2] Unless otherwise stated, all emphasis in bold and italics hereinafter is added, and all footnotes are omitted.

BLOOMBERG NEWS revealed the ***FBI investigation has been ongoing*** "***for more than a year***" ***and that the Department of Justice had confirmed 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.'" The report explained that, while some device owners willingly install proxy services, "[i]n other instances, ***devices are enrolled into residential proxy networks without their owners' knowledge,***" and "users may not even notice the uninvited proxy internet squatters until the police come to their door investigating cybercrime coming from the home."

8. On this news, the Company's share price fell $3.27 or 51.50%, to close at $3.08 on July 6, 2026, on unusually heavy trading volume.

9. Throughout the Class Period, Defendants made materially false and/or misleading statements, as well as failed to disclose material adverse facts about the Company's business, operations, and prospects. Specifically, Defendants failed to disclose to investors: (1) the Company's NetNut business was operating in connection with the Popa botnet which compromised devices with malicious software; (2) the Company's description of the manner in which its NetNut operations collected revenue were false and/or misleading; (3) as a result of the foregoing, the Company's NetNut revenue was inflated by potentially illegal sources; and (4) that, as a result of the foregoing, Defendants' positive statements about the Company's business, operations, and prospects were materially misleading and/or lacked a reasonable basis.

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

JURISDICTION AND VENUE

11. The claims asserted herein arise under 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).

12. 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).

13. 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)). Substantial acts in furtherance of the alleged fraud or the effects of the fraud have occurred in this Judicial District. Many of the acts charged herein, including the dissemination of materially false and/or misleading information, occurred in substantial part in this Judicial District.

14. In connection with the acts, transactions, and conduct alleged herein, Defendants directly and indirectly used the means and instrumentalities of interstate commerce, including the United States mail, interstate telephone communications, and the facilities of a national securities exchange.

PARTIES

15. Plaintiff ____, as set forth in the accompanying certification, incorporated by reference herein, purchased Alarum securities during the Class Period, and suffered damages as a result of the federal securities law violations and false and/or misleading statements and/or material omissions alleged herein.

16. Defendant Alarum is incorporated under the laws of the State of Israel with its principal executive offices located in Tel Aviv, Israel. Alarum's American Depository Shares ("ADS") trade on the NASDAQ exchange under the symbol "ALAR."

17. Defendant Shachar Daniel ("Daniel") was the Company's Chief Executive Officer ("CEO") at all relevant times.

18. Defendant Shai Avnit ("Avnit") was the Company's Chief Financial Officer ("CFO") at all relevant times.

19. Defendants Daniel and Avnit (together, the "Individual Defendants"), because of their positions with the Company, possessed the power and authority to control the contents of the Company's reports to the SEC, press releases and presentations to securities analysts, money and portfolio managers and institutional investors, i.e., the market. The Individual Defendants were provided with copies of the Company's reports and press releases alleged herein to be misleading prior to, or shortly after, their issuance and had the ability and opportunity to prevent their issuance or cause them to be corrected. Because of their positions and access to material non-public information available to them, the Individual Defendants knew that the adverse facts specified herein had not been disclosed to, and were being concealed from, the public, and that the positive representations which were being made were then materially false and/or misleading. The Individual Defendants are liable for the false statements pleaded herein.

SUBSTANTIVE ALLEGATIONS

Background

20. Alarum provides web data collection and proxy services. As of December 31, 2025, the Company has one operating and reportable segment: the Web Data Collection segment. This segment is powered by its subsidiary, NetNut Ltd. ("NetNut"). Alarum acquired NetNut in 2019. Alarum heavily invested in its infrastructure, and by mid-2023, Alarum shifted its main focus strictly to NetNut's operations. NetNut purports to provide tools to gather, extract, and analyze large-scale structured data from public online sources.

Materially False and Misleading

Statements Issued During the Class Period

21. The Class Period begins on March 29, 2022. On that day, Alarum issued a press release announcing its financial results for the fourth quarter and year ended December 31, 2021. The press release described the Company as an alleged "***provider of cyber-security and privacy solutions***" and touted the Company's "***record financial results***" including quarterly revenue of approximately $3.8 million and annual revenue of approximately $10.3 million. The press release further alleged the Company's success was due to "***strong organic growth of [the Company's] privacy business as well as by [the Company's] penetration into the consumer market.***" Specifically, the press release stated as follows, in relevant part:

> Safe-T Group Ltd. (Nasdaq, TASE: SFET) ("Safe-T" or the "Company"), a ***global provider of cyber-security and privacy solutions to consumers and enterprises,*** today announced record financial results for the three-month period and the year ended December 31, 2021.
>
> ● ***Revenues for the three months ended December 31, 2021, reached a quarterly record high of $3,773,000, an increase of 191%*** compared to the three-month period ended December 31, 2020. Revenues for the full year ended December 31, 2021, reached an annual record $10,281,000, an increase of more than 110% compared to results reported for the full year ended December 31, 2020. Annual and quarterly revenues exceeded the Company's previously announced preliminary estimated revenues of $10 million and $3.6 million, respectively.
>
> ● Gross profit for the three-month period ended December 31, 2021, amounted to $2,105,000, an increase of 335% compared to the corresponding period in 2020. Gross profit for the full year ended December 31, 2021, amounted to $5,136,000, an increase of 115% compared to the full year ended December 31, 2020.
>
> Shachar Daniel, Chief Executive Officer of Safe-T, said, "We are proud of our ***record results*** in fiscal 2021, lifted by ***strong organic growth of our privacy business as well as by our penetration into the consumer market, together resulting in record revenues crossing the $10 million annual mark for the first time***. Our business is expanding quarter-over-quarter and year-over-year, ***driven by growing interest in cybersecurity and privacy by consumers***, small and midsized businesses, and enterprises, reinforcing the value of having diverse and complementary offerings.

22. On March 29, 2022, the Company submitted its annual report for the fourth quarter and year ended December 31, 2021, on a Form 20-F filed with the SEC (the "FY21 20-F"). The FY21 20-F affirmed the previously reported financial results, and further reported the Company's alleged revenue by source, including that revenue grew "***due to an increase of $2,427,000 (63%) to $6,266,000 in SaaS revenue in the enterprise privacy segment, generated by NetNut and NetNut Networks, compared to $3,839,000 of such revenue in 2020***." Specifically, the FY21 20-F stated as follows, in relevant part:

	Year ended December 31,	
U.S. dollars in thousands	**2021**	**2020**
SaaS	7,328	3,839
Advertising services	2,325	-
Software licenses	227	447
Software support services	401	587
Other services	-	13
Total Revenues	10,281	4,886

> Our revenues for the year ended December 31, 2021 amounted to $10,281,000, representing an increase of $5,395,000 or 110%, compared to $4,886,000 for the year ended December 31, 2020. The increase is mainly attributed to the $3,387,000 of consumer cybersecurity and privacy revenues generated by CyberKick following its acquisition by us on July 4, 2021, of which $2,325,000 are advertising services and $1,062,000 are SasS. ***Revenues grew also due to an increase of $2,427,000 (63%) to $6,266,000 in SaaS revenue in the enterprise privacy segment, generated by NetNut and NetNut Networks, compared to $3,839,000 of such revenue in 2020,*** which included revenues of NetNut Networks only since its acquisition on December 8, 2021.

23. The FY21 20-F also purported to describe the Company's business model and revenue sources as "***generate[ing] SaaS revenues, advertising services revenues, software licenses revenues, software support services and other services revenues.***" The FY21 20-F further purported to describe NetNut as providing "***enterprise privacy services***" including that NetNut's "***service network is based on partnership agreements with tens of ISPs which enables our***

customers to access the internet using the ISPs' networks." Specifically, the FY21 20-F stated as follows, in relevant part:

> **Our Business Model**
>
> ***We generate SaaS revenues, advertising services revenues, software licenses revenues, software support services and other services revenues.***
>
> ***The SaaS revenues are generated when customers are subscribing to our enterprise and consumer privacy and security platforms and paying for the packages they choose.*** The packages are usually for the earlier of one day to three months or maximum bandwidth usage in the enterprise privacy segment, and for a month or a year in the consumers privacy and security segments. Our revenue is recognized on a straight-line basis over the package period.
>
> We generate revenues on the consumer privacy arena also from providing advertising services to enterprise customers, using marketing tools on various sites in order to persuade the user to acquire the enterprise customers' privacy products. Revenue is recognized at the point in time when a user purchased an application or software of a customer.
>
> We offer our enterprise privacy customers an on-premise solution (proxy-in-a-box), for enterprise privacy customers who wish to deploy and maintain the proxy network by themselves. The revenues from selling such solutions are recognized upon delivery of the system to the customer. No systems were sold during 2021.
>
> * * *
>
> **NetNut Ltd.** is our wholly-owned subsidiary incorporated in Israel. NetNut operates in the field of ***enterprise privacy services, which enables customers to collect data anonymously at any scale from any public sources over the web using a unique hybrid network.***
>
> * * *
>
> ***Following the acquisition of NetNut in June 2019, as further detailed below, we launched our enterprise privacy service. The service network is based on partnership agreements with tens of ISPs which enables our customers to access the internet using the ISPs' networks through millions of end points globally, and collect valuable data for their needs.*** The service's performance and scalability are enhanced by our proprietary proxy traffic optimization and routing technology.

24. The FY21 20-F purported to warn of risks which "***could***" or "***may***" negatively impact the Company, including "***[i]f we experience an actual or perceived breach of our network***

and our internal systems, it could adversely affect the market perception of our products and services." The FY21 20-F further purported to warn that "***[w]e generate a portion of our revenues from our products and services because they enable our customers to achieve and maintain compliance with certain government regulations***" but "***changes in regulations may impact the means or ability to provide such solutions.***" Specifically, the FY21 20-F stated as follows, in relevant part:

> ***If our internal network system is compromised by cyber attackers or other data thieves, or if our hosting and infrastructure fails, public perception of our products and services will be harmed.***
>
> We will not succeed unless the marketplace is confident that we provide effective cybersecurity protection. ***As part of our offered solutions, we provide zero trust access products through a cybersecurity specialist reseller*** (see "Item 4. B. — Business Overview" for additional information), and as such we may be an attractive target for attacks by cyber attackers or other data thieves since a breach of our network could provide data information regarding not only us, but potentially regarding the customers who purchased our solutions. Further, we may be targeted by cyber terrorists because we are an Israeli company. ***If we experience an actual or perceived breach of our network and our internal systems, it could adversely affect the market perception of our products and services.***
>
> * * *
>
> ***If our products fail to help our customers achieve and maintain compliance with certain government regulations and industry standards, our business and results of operations could be materially and adversely affected.***
>
> ***We generate a portion of our revenues from our products and services because they enable our customers to achieve and maintain compliance with certain government regulations and industry standards, and we expect that will continue for the foreseeable future.*** Examples of industry standards and government regulations include the European Union General Data Protection Regulation, or GDPR; the Payment Card Industry Data Security Standard, or PCI-DSS; the Health Insurance Portability and Accountability Act, or HIPAA; the Sarbanes-Oxley Act; the Gramm-Leach-Bliley Act, or GLBA; and the international banking regulations of the Basel Committee on Bank Supervision.
>
> On the enterprise privacy side of our business, we primarily engage directly with ISPs in order to gain access to their networks. The legality of scraping publicly available web data was reaffirmed by the Ninth Circuit Court of Appeals (hiQ vs LinkedIn) in late 2019, but the way in which some of the automated software

programs are built is still questionable, and ***changes in regulations may impact the means or ability to provide such solutions.***

25. On March 31, 2023, the Company issued a press release announcing its financial results for the fourth quarter and year ended December 31, 2022. The press release described the Company as an alleged "***provider of enterprise and consumers internet access solutions,***" and touted the Company's "***fourth consecutive year and the eighth consecutive quarter of exponential growth***" including quarterly revenue of approximately $5.2 million and annual revenue of approximately $18.8 million. The press release alleged the Company's success was due to "***the strength of [the Company's] business model.***" The press release also touted NetNut's results, including its alleged "***Anti-fraud solution***." Specifically, the press release stated as follows, in relevant part:

> Alarum Technologies Ltd. (Nasdaq, TASE: ALAR) ("Alarum" or the "Company"), a ***global provider of enterprise and consumers internet access solutions***, today announced record financial results for the three months and year ended December 31, 2022.
>
> Key highlights for the three months and year ended December 31, 2022:
>
> ● ***Revenues for the three months ended December 31, 2022, reached a record high of $5.2 million, an increase of approximately 37% compared to the three months ended December 31, 2021.***
>
> ● ***Full year 2022 revenues totaled a record of $18.8 million, an increase of approximately 83% compared to 2021.***
>
> ● NetNut Ltd. ("NetNut"), the Company's internet access company for organizations, became cashflow positive.
>
> ● Net loss and adjusted EBITDA loss for the fourth quarter of 2022 totaled $2.9 million and $1.7 million, respectively, a decrease of approximately 36% and 55%, respectively, compared to the equivalent quarter of 2021.
>
> "We are proud to announce a ***fourth consecutive year and the eighth consecutive quarter of exponential growth.*** We are also pleased to share that we are making excellent progress in accelerating our path towards profitability – in addition to our revenue growth, and through careful planning, we have been able to significantly reduce our losses and burn rate, a trend that continued into the first quarter of 2023

with even greater reduction compared to the fourth quarter of 2022," said Shachar Daniel, Chief Executive Officer of Alarum.

"***These impressive milestones were achieved with hard work and our commitment to deliver great value to our customers.*** We have invested in product improvements, which have resulted in increased customer retention and lower consumer acquisition costs. ***We are extremely proud of our enterprise internet access arm, NetNut, that is positioning itself as a leading brand in its field and has become profitable in the last quarter with a growing customer base and revenues.***

* * *

"Overall, ***these results demonstrate the strength of our business model*** and our commitment to delivering long-term value for our stakeholders. Looking ahead, we remain steadfast in executing our long-term strategy and are committed to delivering sustainable growth and value for our stakeholders. We are confident that our financial position and resilient and scalable business model will allow us to remain on track to building a leading company in our space," Mr. Daniel concluded.

* * *

- Cybersecurity: ***NetNut enabled its new enterprise cybersecurity customers to identify potential cyber-attacks.***

- NetNut launched its new mobile IP Proxy network with sales to the first three customers.

- NetNut's network doubled usage volume within one month with more than 36 billion requests processed.

- E-commerce: NetNut successfully gained increased traction among E-commerce customers in preparation for November 2022 shopping events.

- Anti-fraud solution: ***NetNut won three new leading customers to use its advanced solution for advertising fraud detection, mitigation, and prevention.***

26. On March 31, 2022, the Company submitted its annual report for the fourth quarter and year ended December 31, 2023, on a Form 20-F filed with the SEC (the "FY22 20-F"). The FY22 20-F affirmed the previously reported financial results, and further reported the Company's alleged revenue by source, including that revenue grew "***due to an increase of $2,214,000 (35%) to $8,479,000 in SaaS revenue in the enterprise access segment, generated by NetNut and***

NetNut Networks in 2022, compared to $6,265,000 of such revenue in 2021." Specifically, the FY22 20-F stated as follows, in relevant part:

U.S. dollars in thousands	Year ended December 31, 2022	2021
SaaS	11,850	7,328
Advertising services	6,699	2,325
Software licenses	28	227
Software support services	202	401
Total Revenues	18,779	10,281

* * *

Our revenues for the year ended December 31, 2022 amounted to $18,779,000, representing an increase of $8,498,000, or 83%, compared to $10,281,000 for the year ended December 31, 2021. The increase is mainly attributed to a $6,681,000 increase to $10,070,000 (197%) in the consumer access segment revenues generated by CyberKick compared to 2021, where the revenues were consolidated only from its acquisition on July 4, 2021. ***Revenues grew also due to an increase of $2,214,000 (35%) to $8,479,000 in SaaS revenue in the enterprise access segment, generated by NetNut and NetNut Networks in 2022, compared to $6,265,000 of such revenue in 2021.***

27. The FY22 20-F also purported to describe the Company's business model and revenue sources, including that it "***generate[s] primarily SaaS revenues and advertising services revenues.***" The FY22 20-F further purported to describe NetNut as providing "***internet access services for enterprises, which enables customers to collect data anonymously***" including that NetNut's "***service is based on partnership agreements with tens of ISPs around the world***." Specifically, the FY22 20-F stated as follows, in relevant part:

Our Business Model

We generate primarily SaaS revenues and advertising services revenues. We also generate immaterial software licenses revenues and software support services revenues in the enterprise security segment through TerraZone, a third party provider (see also "Item 4B- Business Overview").

The SaaS revenues are generated when customers are subscribing to our enterprise and consumer access platforms and paying for the packages they

choose. The packages are usually for the earlier of one day to three months or maximum bandwidth usage in the enterprise privacy segment, and for a month or a year in the consumers access segment. Our revenue is recognized on a straight-line basis over the package period.

We generate revenues on the consumer access arena also from providing advertising services to enterprise customers, using marketing tools on various sites in order to persuade the user to acquire the enterprise customers' privacy products. Revenue is recognized at the point in time when a user purchased an application or software of a customer.

* * *

NetNut Ltd. is our wholly-owned subsidiary incorporated in Israel. ***NetNut operates in the field of internet access services for enterprises, which enables customers to collect data anonymously at any scale from any public sources over the web using a unique hybrid network.***

* * *

Following our acquisition of NetNut in June 2019, as further detailed below, we launched our web data collection service. ***The service is based on partnership agreements with tens of ISPs around the world, as well as our proprietary software deployed at data centers and devices which enable our customers to access the internet through millions of end points globally, and collect valuable data for their needs.*** The service's performance and scalability are enhanced by our proprietary proxy traffic optimization and routing technology.

Customers in the web data collection market use the proxy service for various needs and for a wide variety of use cases, as mentioned above. To address all these use cases, different types of web data collection services are needed. For some of the use cases, the web data collection service needs to be fast and stable, and allow customers to use the same IP address for long time periods, while for others, the most important factor of a web data collection service is its ability to provide a different IP address for each request in order to be able to get a full picture of the collected data. For these reasons, providers in the web data collection market are required to provide a wide selection and web data collection services types. We have invested heavily in the last year in expanding our offering in order to become a leading provider in this market.

The uniqueness of our web data collection service is based on the fact that unlike our competitors that provide predominantly host-based solutions, which require installation of software on third-party uncontrolled end user devices, we support not only running software on end user devices, but also routing the customer's traffic through residential routers of our ISP partners.

28. The FY22 20-F purported to warn of risks which "***could***" or "***may***" negatively impact the Company, including "***[i]f we experience an actual or perceived breach of our network and our internal systems, it could adversely affect the market perception of our products and services.***" The FY22 20-F further purported to warn that "***help our customers achieve and maintain compliance with certain government regulations***" but "***changes in regulations may impact the means or ability to provide such solutions.***" Specifically, the FY22 20-F stated as follows, in relevant part:

> ***If our internal network system is compromised by cyber attackers or other data thieves, or if our hosting and infrastructure fails, public perception of our products and services will be harmed.***
>
> 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. ***If we experience an 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. With respect to the enterprise access services and consumers services, if we will 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.
>
> * * *
>
> ***If our products fail to help our customers achieve and maintain compliance with certain government regulations and industry standards, our business and results of operations could be materially and adversely affected.***
>
> On the enterprise access side of our business, ***we primarily engage directly with ISPs in order to gain access to their networks.*** The legality of scraping publicly available web data was reaffirmed by the Ninth Circuit Court of Appeals (hiQ vs LinkedIn) in late 2019, but the way in which some of the automated software

programs are built is still questionable, and ***changes in regulations may impact the means or ability to provide such solutions.***

29. On January 9, 2024, the Company issued a press release announcing certain "key financial metrics guidance for the three months and twelve months ended on December 31, 2023." The press release touted the Company's "Revenue for the fourth quarter of 2023 is estimated at more than $7 million, representing the ***highest quarterly revenues achievement to-date.***" The Company also attributed its results to the Company's "***strategic shift towards focusing on growth and business activity of its wholly owned subsidiary, NetNut***." Specifically, the press release stated as follows, in relevant part:

> Based on a preliminary, unaudited review, Alarum anticipates reporting strong performance for the fourth quarter of 2023 and the entire year of 2023, highlighting accelerated operating and business growth:
>
> - ***Revenue for the fourth quarter of 2023 is estimated at more than $7 million, representing the highest quarterly revenues achievement to-date*** and an increase of 35% compared to the same period in 2022.
>
> - In the fourth quarter of 2023, the Company generated approximately $2.8 million in cashflow from operating activities, compared to a negative cashflow of approximately $1.8 million for the same period in 2022.
>
> - Total expected revenue for 2023 is estimated at $26.5 million, an increase of approximately 41% compared to total revenue of $18.8 million in 2022.
>
> - Cash and cash equivalents balance as of December 31, 2023, amounted to approximately $10.8 million.
>
> ***In 2023, the Company made a strategic shift towards focusing on growth and business activity of its wholly owned subsidiary, NetNut Ltd. ("NetNut"). As a result, the Company experienced a positive impact throughout its entire business aspects, which not only led to a net profit in the third quarter of 2023 but also resulted in record revenues in the fourth quarter and the entire year of 2023.*** NetNut's revenue for the fourth quarter of 2023 are estimated at $6.8 million, representing an increase of 150% compared to the equivalent period in 2022, and its estimated 2023 annual revenue ramped up to a record of more than $21 million, also an increase of 150% compared to full year 2022.

* * *

> "The amazing results we achieved in the fourth quarter of 2023 emphasize the positive impact advanced by the strategic business changes we implemented during 2023, which are fostering growth and success. Following our decision to focus on improved profitability and reduce investments in the consumer segment, we anticipated that most of our fourth-quarter revenues will be generated by NetNut. These revenues alone surpass the combined revenue of both NetNut and consumer segments from previous periods," Daniel added.

30. On March 14, 2024, Alarum issued a press release announcing its financial results for the fourth quarter and year ended December 31, 2023. The press release described the Company as an alleged "***provider of internet access and data collection solutions***" and touted the Company's "***record financial results***" including quarterly revenue of approximately $7.1 million and annual revenue of approximately $26.5 million, includin NetNut revenue of $21.3 million. The press release further alleged the Company's success was due to the Company's decision to "***scale down other activities and focus on NetNut's operations***." Specifically, the press release stated as follows, in relevant part:

> Alarum Technologies Ltd. (Nasdaq, TASE: ALAR) ("Alarum" or the "Company"), a global provider of internet access and data collection solutions, today announced record financial results for the three months and full year periods, ended December 31, 2023.
>
> Key highlights for the three months and year ended December 31, 2023:
>
> * * *
>
> - ***Revenues from continuing operations for the three months ended December 31, 2023, reached a record high of $7.1 million, an increase of approximately 39% compared to the three months ended December 31, 2022.***
>
> - ***Revenues from continuing operations for the full year of 2023 totaled $26.5 million, an increase of approximately 43% compared to $18.6 million in 2022.***
>
> - ***NetNut's 2023 full year revenue amounted to $21.3 million, reflecting growth of over 150% year-over-year, compared to $8.5 million in revenues for 2022.***
>
> "I am proud to share the most successful quarter in the Company's history, as revenue, net profit and Adjusted EBITDA, all meaningfully exceeded results from

the previous quarter. ***We delivered efficient operational execution following our decision, in the second quarter of 2023, to scale down other activities and focus on NetNut's operations,***" said Shachar Daniel, Alarum's Chief Executive Officer.

31. On March 14, 2024, the Company submitted its annual report for the fourth quarter and year ended December 31, 2023, on a Form 20-F filed with the SEC (the "FY23 20-F"). The FY23 20-F affirmed the previously reported financial results, and further reported the Company's alleged revenue by source, including that the revenue "***increase is attributed to a $12.8 million increase from $8.5 million to $21.3 million (151%) in the enterprise internet access segment revenues generated by NetNut compared to 2022.***" Specifically, the FY23 20-F stated as follows, in relevant part:

U.S. dollars in millions	Year ended December 31, 2023	2022
Software as a Service	23.7	11.9
Advertising services	2.8	6.7
Total Revenues	**26.5**	**18.6**

* * *

Our revenues for the year ended December 31, 2023, amounted to $26.5 million, representing an increase of $7.9 million, or 42%, compared to $18.6 million for the year ended December 31, 2022. ***The increase is attributed to a $12.8 million increase from $8.5 million to $21.3 million (151%) in the enterprise internet access segment revenues generated by NetNut compared to 2022.*** These increases were partially offset by a $4.8 million decrease (48%) in the consumer internet access segment revenues, from $10.0 million to $5.2 million, due to the cessation of the advertising services in mid-2023 and the scale down in the consumer product operations and revenues.

32. The FY23 20-F also purported to describe the Company's business model and revenue sources as "***generat[ing] SaaS revenues when customers are subscribing to our enterprise and consumer access platforms and paying for the packages they choose***" The FY23 20-F further purported to describe NetNut as "***operat[ing] in the field of internet access and web data collection services,***" including that NetNut's "***services are based on partnership agreements***

with tens of ISPs around the world," Specifically, the FY23 20-F stated as follows, in relevant part:

> **Our Business Model**
>
> ***We generate SaaS revenues when customers are subscribing to our enterprise and consumer access platforms and paying for the packages they choose.*** The packages are usually for the earlier of one to twelve months or maximum bandwidth usage in the enterprise access segment, and for a month or a year in the consumers access segment. Our revenue is recognized on a straight-line basis over the package period.
>
> * * *
>
> **NetNut Ltd.** is our wholly owned subsidiary incorporated in Israel. NetNut ***operates in the field of internet access and web data collection services,*** which enables customers to collect data anonymously at any scale from any public sources over the web using a unique hybrid network.
>
> * * *
>
> Following our acquisition of NetNut in June 2019, we launched our web data collection services. ***The services are based on partnership agreements with tens of ISPs around the world, as well as our proprietary software deployed at data centers and devices which enable our customers to access the internet through millions of end points globally and collect valuable data for their needs.*** The services' performance and scalability are enhanced by our proprietary proxy traffic optimization and routing technology.

33. The FY23 20-F purported to warn of risks which "***could***" or "***may***" negatively impact the Company, including "***[i]f we experience an actual or perceived breach of our network and our internal systems, it could adversely affect the market perception of our products and services.***" The FY23 20-F further purported to warn that the Company helps customers "***achieve and maintain compliance with certain government regulations*** " but "***changes in regulations may impact the means or ability to provide such solutions.***" Specifically, the FY23 20-F stated as follows, in relevant part:

> ***If our network system is compromised by cyber attackers or other data thieves, or if our hosting and infrastructure fails, public perception of our products and services will be harmed.***

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. If we experience an 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 our products fail to help our customers achieve and maintain compliance with certain government regulations and industry standards, our business and results of operations could be materially and adversely affected.

On the enterprise access side of our business, we primarily engage directly with ISPs in order to gain access to their networks. The legality of scraping publicly available web data was first upheld in late 2019, and then reaffirmed by the Ninth Circuit Court of Appeals (hiQ vs LinkedIn) in April 2022. We also note that X Corp (formerly Twitter) has launched several complaints on scraping of its platform, separately bringing three lawsuits against alleged scrapers of its site. The Meta v. Bright Data case may serve as a precedent. 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.***

34. On March 20, 2025, the Company issued a press release announcing its financial results for the fourth quarter and year ended December 31, 2024. The press release described the Company as an alleged "***provider of web data collection solutions,***" and touted the Company's "***landmark year***" including quarterly revenue of approximately $7.4 million and annual revenue of approximately "record" $31.8 million, including web data collection revenue of $30.9 million. The press release further alleged the Company's success was due to Alarum having "***successfully***

executed our strategic vision, to focus on data collection." Specifically, the press release stated as follows, in relevant part:

> Alarum Technologies Ltd. (Nasdaq, TASE: ALAR) ("Alarum" or the "Company"), a global ***provider of web data collection solutions,*** today announced financial results for the fourth quarter and full year ended December 31, 2024.
>
> Shachar Daniel, Chief Executive Officer of Alarum, said: "***2024 was a landmark year for Alarum, as we successfully executed our strategic vision, to focus on data collection.*** This transformation comes at a time when AI is reshaping the world at an unprecedented pace. As data fuels intelligence, the companies that will lead this revolution are those that anticipate change, build a strong foundation, and position themselves for long-term success. This is exactly what we are striving for - taking it step by step."
>
> * * *
>
> **Fourth Quarter and Full Year 2024 Financial Analysis**
>
> - ***Revenue in Q4 2024 grew 4% year-over-year to $7.4 million (Q4 2023: $7.1 million). The increase is attributed to our NetNut web data collection business,*** which grew 7% to $7.2 million in Q4 2024, up from $6.7 million in Q4 2023. ***Revenue for the whole year 2024 grew 20%, rising to a record of $31.8 million*** (2023: $26.5 million). ***The Web Data Collection revenue reached a Company record $30.9 million*** in 2024, achieving 45% year-over-year growth (2023: $21.3 million).

35. On March 20, 2025, the Company submitted its annual report for the fourth quarter and year ended December 31, 2024, on a Form 20-F filed with the SEC (the "FY24 20-F"). The FY24 20-F affirmed the previously reported financial results, and further reported the Company's alleged revenue by source, including that the revenue "***increase is attributed to a $9.6 million increase from $21.3 million to $30.9 million (45%) in the web data collection segment revenues compared to 2023 due to an increase in sales volume.***" Specifically, the FY24 20-F stated as follows, in relevant part:

	Year ended December 31,	
U.S. dollars in millions	**2024**	**2023**
Software as a Service	31.8	23.7
Advertising services	*	2.8
Total Revenues	**31.8**	**26.5**

* Less than $0.1

Our revenues for the year ended December 31, 2024, amounted to $31.8 million, representing an increase of $5.3 million, or 20%, compared to $26.5 million for the year ended December 31, 2023. ***The increase is attributed to a $9.6 million increase from $21.3 million to $30.9 million (45%) in the web data collection segment revenues compared to 2023 due to an increase in sales volume***.

36. The FY24 20-F also purported to describe the Company's business model and revenue sources, including that the Company "***generate[s] SaaS revenues when customers subscribe to our web data collection and consumer internet access platforms and pay for the packages they choose***" The FY24 20-F further purported to describe NetNut as providing "***secured, fast, and anonymous IPPN Solutions to our business customers***" and that NetNut's "***services are based on partnership agreements with tens of ISPs around the world.***" Specifically, the FY24 20-F stated as follows, in relevant part:

Our Business Model

Alarum is a global provider of web data collection solutions.

We currently operate in one segment: web data collection.

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.

* * *

We generate SaaS revenues when customers subscribe to our web data collection and consumer internet access platforms and pay for the packages they choose. In the web data collection segment packages are usually used for a period of one to twelve months, or for a shorter period if the maximum bandwidth was utilized. In the consumer internet access platform, packages are primarily used for a period of

one month. Our revenue is recognized on a straight-line basis over the package period.

* * *

NetNut Ltd. is our wholly owned subsidiary incorporated in Israel. NetNut operates in the field of web data collection services, which ***enables customers to collect data anonymously at any scale from any public sources over the web using a unique hybrid network.***

* * *

Following our acquisition of NetNut in June 2019, we launched our web data collection services. ***The services are based on partnership agreements with tens of ISPs around the world,*** as well as our proprietary software deployed at data centers and devices which enable our customers to access the internet through millions of end points globally and collect valuable data for their needs. The services' performance and scalability are enhanced by our proprietary proxy traffic optimization and routing technology.

37. The FY24 20-F purported to warn of risks which "***could***" or "***may***" negatively impact the Company, including "***[i]f we experience an actual or perceived breach of our network and our internal systems, it could adversely affect the market perception of our products and services.***" The FY23 20-F further purported to warn that "***potential for changes in regulations that could affect the ability to provide such solutions.***" Specifically, the FY24 20-F stated as follows, in relevant part:

If our internal network system is compromise 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.

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***.

* * *

If our products fail to ensure customer compliance with government regulations and industry standards, our business and results could be materially impacted.

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.***

38. On March 19, 2026, the Company issued a press release announcing its financial results for the fourth quarter and year ended December 31, 2025. The press release described the Company as an alleged "provider of web data collection solutions" and touted the Company's quarterly revenue of approximately $11.8 million and annual revenue of approximately $40.7 million. The press release further alleged the Company's success was due to a "***expanding workloads from large-scale artificial intelligence ("AI") customers and broader adoption of the Company's data infrastructure products.***." Specifically, the press release stated as follows, in relevant part:

Alarum Technologies Ltd. (Nasdaq: ALAR, TASE: ALAR) ("Alarum" or the "Company"), a global provider of web data collection solutions, today announced its financial results for the fourth quarter and full year ended December 31, 2025.

Financial Highlights of Full Year 2025

- ***2025 revenues of $40.7 million***, up 28% year-over-year compared to $31.8 million in 2024.

* * *

- ***Fourth quarter of 2025 revenues of $11.8 million***, up 60% year-over-year.

* * *

- Revenue growth in the quarter was driven primarily by ***expanding workloads from large-scale artificial intelligence ("AI") customers and broader adoption of the Company's data infrastructure products.***

39. On March 19, 2026, the Company submitted its annual report for the fourth quarter and year ended December 31, 2025, on a Form 20-F filed with the SEC (the "FY25 20-F"). The FY25 20-F affirmed the previously reported financial results, and further reported the Company's alleged revenue by source, including that revenue "***increase is attributed to strong demand for the Company's services by a large-scale customer building foundational AI models, as well as increased sales of new products. Specifically, data collection solutions and data sets together generated $11.1 million in revenues, compared to only $0.6 million in 2024.***" Specifically, the FY25 20-F stated as follows, in relevant part:

	Year ended December 31,	
U.S. dollars in millions	**2025**	**2024**
Web Data Collection		
SaaS revenue:		
IPPN solutions	29.2	30.3
Data collection solutions	6.1	0.6
Total SaaS revenue	35.3	30.9
Data sets revenue	5.0	-
Total Web Data Collection revenue	40.3	30.9
Other revenue	0.4	0.9
Total Revenues	**40.7**	**31.8**

* * *

Our revenues for the year ended December 31, 2025, amounted to $40.7 million, representing an increase of $8.9 million, or 28%, compared to $31.8 million for the year ended December 31, 2024. ***This increase is attributed to strong demand for***

the Company's services by a large-scale customer building foundational AI models, as well as increased sales of new products. Specifically, data collection solutions and data sets together generated $11.1 million in revenues, compared to only $0.6 million in 2024.

40. The FY25 20-F also purported to describe the Company's business model and revenue sources, including that the Company "***generate[s] primarily SaaS revenue from customers utilizing our solutions, which consists mainly of subscription fees and usage-based fees.***" The FY25 20-F further purported to describe NetNut as operating "***[t]hrough partnerships with tens of ISPs worldwide.***" Specifically, the FY25 20-F stated as follows, in relevant part:

> ***We generate primarily SaaS revenue from customers utilizing our solutions, which consists mainly of subscription fees and usage-based fees.***
>
> Our subscriptions are offered on a periodic basis, typically yearly or monthly, and include primarily a fixed price for a pre-defined data volume or speed. Revenue from subscription-based contracts is recognized on a straight-line basis over the term of the contract, generally beginning on the date when the solution is made available to the customer.
>
> * * *
>
> NetNut Ltd. is our wholly owned subsidiary incorporated in Israel. NetNut operates in the field of web data collection solutions, which ***enables customers to collect data anonymously at any scale from any public sources over the web using a unique hybrid network.***
>
> * * *
>
> Following our acquisition of NetNut in June 2019, we strengthened our global proxy network. ***Through partnerships with tens of ISPs worldwide and our proprietary software deployed on data centers and devices, we provide customers with access to millions of global endpoints.*** Our proprietary proxy traffic optimization and routing technology ensures high performance and scalability, enabling reliable, uninterrupted access to the web for a wide range of use cases. Built on top of our robust proxy infrastructure, our web data collection solutions allow customers to gather valuable public web data at scale. These tools enable access to websites protected by anti-bot technologies, delivering both structured and raw data in real-time. Our solutions include customizable scrapers, automated collection workflows, and pre-processed datasets, empowering customers to retrieve, aggregate, and use web data efficiently while bypassing common anti-bot restrictions.

41. The FY25 20-F purported to warn of risks which "could" or "may" negatively impact the Company, including "***if we experience another actual or perceived breach of our network and our internal systems, it could adversely affect the market perception of our solutions and products***." The FY25 20-F further purported to warn that "***[r]egulatory or judicial developments may materially affect the methods or feasibility of providing certain data-driven solutions.***" Specifically, the FY25 20-F stated as follows, in relevant part:

> ***If our internal network system is compromise by cyber attackers or other malicious cyber activity, or if our hosting and infrastructure fails, public perception of our solutions and products will be harmed.***
>
> 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 solutions and products.***
>
> * * *
>
> ***If our products fail to ensure customer compliance with government regulations and industry standards, our business and results could be materially impacted.***
>
> The legality of scraping publicly available web data was upheld in late 2019, when the Ninth Circuit Court of Appeals ruled in hiQ Labs, Inc., or hiQ, v. LinkedIn Corporation that scraping publicly accessible data did not violate the Computer Fraud and Abuse Act. However, the hiQ litigation did not ultimately result in a definitive nationwide rule. The U.S. Supreme Court vacated an earlier Ninth Circuit opinion in 2021, and although the Ninth Circuit reaffirmed its position in 2022, hiQ later entered bankruptcy and the case was ultimately resolved without a final merits ruling. As a result, the hiQ decisions remain influential but create continued legal uncertainty rather than a settled precedent. More broadly, large online platforms have intensified their efforts to restrict scraping. For example, X Corp. (formerly Twitter) has filed multiple lawsuits against parties accused of scraping its platform without consent, and Meta Platforms, Inc. has pursued litigation against Bright Data Ltd., arguing that automated collection of publicly available data violates user agreements and intellectual property rights. Courts have reached mixed conclusions

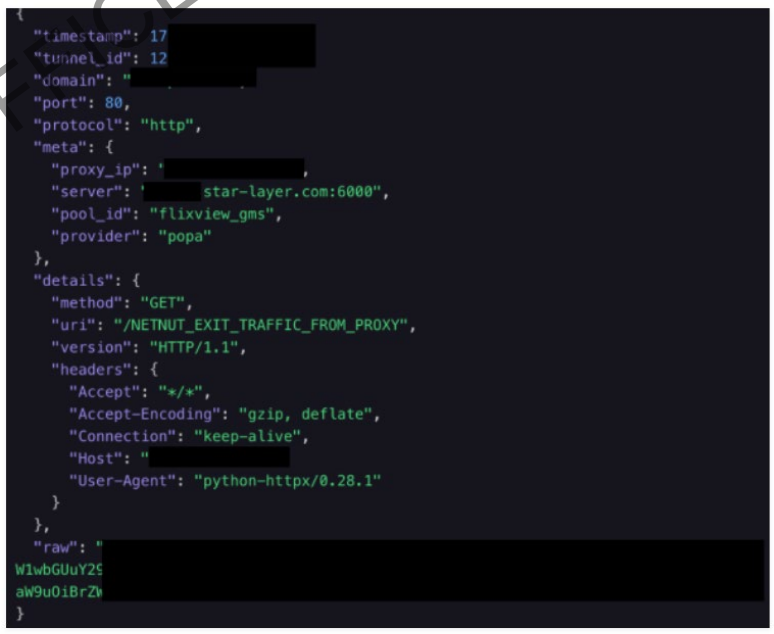
> in these and similar cases, with some rulings supporting contractual limitations on automated access. This trend reflects an increasingly aggressive enforcement posture by major platforms toward data collection activities. As the web continues to evolve as a vast source of information, the debate over data accessibility versus privacy has intensified, including heightened scrutiny of automated software tools, large-scale data collection, and AI-related data sourcing practices. ***Regulatory or judicial developments may materially affect the methods or feasibility of providing certain data-driven solutions.***

42. The above statements identified in ¶¶21-41 were materially false and/or misleading, and failed to disclose material adverse facts about the Company's business, operations, and prospects. Specifically, Defendants failed to disclose to investors: (1) the Company's NetNut business was operating in connection with the Popa botnet which compromised devices with malicious software; (2) the Company's description of the manner in which its NetNut operations collected revenue were false and/or misleading; (3) as a result of the foregoing, the Company's NetNut revenue was inflated by potentially illegal sources; and (4) that, as a result of the foregoing, Defendants' positive statements about the Company's business, operations, and prospects were materially misleading and/or lacked a reasonable basis.

43. On June 18, 2026, after the market closed, popular cybersecurity blog Krebs on Security reported that several security firms had published reports that allegedly linked NetNut with the pervasive botnet Popa. The report stated "***for the past four years,***" "Popa has forced millions of consumer TV boxes to relay Internet traffic linked to advertising fraud, account takeovers, and mass data-scraping efforts." "This week, researchers from multiple security firms concluded that the ***Popa botnet is linked to NetNut, . . . operated by the publicly-traded Israeli firm Alarum Technologies Ltd***." The post further stated that Alarum had provided a statement to Krebs on Security, which said "the [Software Development Kits] at issue are designed to facilitate bandwidth-sharing functionality and do not transform user devices into malware-controlled

systems or otherwise compromise the devices on which they operate." Specifically, the post stated as follows, in relevant part:

> For the past four years, a sprawling Android-based botnet called **Popa** has forced millions of consumer TV boxes to relay Internet traffic linked to advertising fraud, account takeovers, and mass data-scraping efforts. This week, researchers from multiple security firms concluded that the Popa botnet is linked to **NetNut**, a "residential proxy" provider operated by the publicly-traded Israeli firm **Alarum Technologies Ltd** [NASDAQ: ALAR].
>
> Popa is a massive botnet, but by all accounts it is unlike traditional botnets that enlist compromised systems in destructive activities, such as coordinating huge distributed denial-of-service attacks. Rather, Popa appears designed with a singular purpose: Implementing a persistent communications layer capable of registering a device, maintaining long-lived encrypted connections, and opening communication tunnels on demand.
>
> * * *
>
> But in a separate Popa research report released today, the proxy-tracking company **Synthient** said a recent analysis of the Popa SDK revealed outbound traffic clearly associated with NetNut.
>
> "The research team assesses with high confidence that devices running Popa forward traffic from Netnut clients," Synthient wrote. "This proves without a shadow of a doubt that Popa actively continues to be used by NetNut as part of their proxy pool."



Synthient's platform receiving outbound traffic from Popa. Image: Synthient.com.

> Alarum Technologies, NetNut's Tel Aviv-based parent company, said the reports by Synthient and Qurium contained "demonstrably inaccurate assertions and flawed deductions rather than verified facts." Alarum shared a statement saying they reject the basic characterization of the SDKs and technologies discussed in the reports as a "botnet."
>
> "The SDKs at issue are designed to facilitate bandwidth-sharing functionality and do not transform user devices into malware-controlled systems or otherwise compromise the devices on which they operate," the statement reads. "Netnut operates a commercial proxy network and maintains policies, procedures, and technological measures designed to promote lawful and responsible use of its services."
>
> Alarum said NetNut places "significant emphasis on appropriate notice and consent mechanisms, conducts customer due diligence, monitors for potential misuse, and takes steps intended to detect and mitigate suspicious or unauthorized activity."
>
> "This method of operation is supported both by internal procedures and policies, including performing KYC checks and additional due diligence of NetNut's customers, as well as employing various technological measures, designed to assist in identifying and addressing suspected misuse of the network," their statement continued.

44. On this news, the Company's share price fell $0.76 or 8.3%, to close at $8.41 on June 22, 2026, on unusually heavy trading volume.

45. The above statements identified in ¶43 were materially false and/or misleading, and failed to disclose material adverse facts about the Company's business, operations, and prospects. Specifically, Defendants failed to disclose to investors: (1) the Company's NetNut business was operating in connection with the Popa botnet which compromised devices with malicious software; (2) the Company's description of the manner in which its NetNut operations collected revenue were false and/or misleading; (3) as a result of the foregoing, the Company's NetNut revenue was inflated by potentially illegal sources; and (4) that, as a result of the foregoing, Defendants' positive statements about the Company's business, operations, and prospects were materially misleading and/or lacked a reasonable basis.

Disclosures at the End of the Class Period

46. On July 2, 2026, at approximately 2:00 PM EST, REUTERS reported Google had taken action against 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 reportedly "***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." The article stated "NetNut's parent, Israel-based web data provider Alarum Technologies was informed of the ***seizure of some of its domains by the FBI on Thursday***, the company told Reuters." Specifically, the report stated as follows, in relevant part:

> **Google disrupts NetNut proxy network used in malware operations**
>
> July 2 (REUTERS) - Alphabet's 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.

47. On this news, the Company's share price fell $1.67 or 20.81%, to close at $6.35 on July 2, 2026, on unusually heavy trading volume.

48. Then, on July 2, 2026, after the market closed, BLOOMBERG NEWS revealed details of the FBI's investigation into ***NetNut on claims it may have a "role in linking customers' home internet devices without their consent into a network that people can use to disguise their locations"*** via a "software known as Popa that's allegedly used to co-opt people's devices." BLOOMBERG NEWS revealed the ***FBI investigation has been ongoing*** "***for more than a year***" ***and that the Department of Justice had confirmed 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.'" The report explained that, while some device owners willingly install proxy services, "[i]n other instances, ***devices are enrolled into residential proxy networks without their owners' knowledge,***" and "users may not even notice the uninvited proxy internet squatters until the police come to their door investigating cybercrime coming from the home." Specifically, the REUTERS report stated as follows, in relevant part:

> **FBI Probes Whether Alarum Unit Is Behind Co-Opted Home Devices**
>
> * * *
>
> The FBI is investigating whether a subsidiary of the data-collection firm Alarum Technologies Ltd. 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 NEWSNews 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, US Federal Bureau of Investigation 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."

Omer Weiss, corporate legal counsel for Alarum, said in a statement that the company was made aware Thursday that the FBI had seized some of its domains.

"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," Weiss said in the statement.

The FBI declined to comment on the investigation.

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 experts.

"I think of residential proxy like thousands of anonymous strangers sneaking into your home to get unlimited internet access," said Craig Labovitz, head of technology for the network security platform Nokia Deepfield. "Most users may not even notice the uninvited proxy internet squatters until the police come to their door investigating cybercrime coming from the home."

The FBI investigation, which hasn't been previously reported, is part of a broader law enforcement effort to scrutinize the uses of residential proxy networks. Internet service providers and cybersecurity firms alike have warned that the networks have been used to ensnare millions of devices globally.

* * *

Popa in particular can be used to commandeer a device for a proxy network without the owner's consent, according to June analyses by security firms Synthient and Qurium.

Synthient said in its report that NetNut and Popa "share operational infrastructure and telemetry." Qurium said it had "identified multiple technical and historical overlaps" between the technology behind NetNut and that of Popa that are "unlikely to be coincidental."

* * *

Months before researchers from the cybersecurity firms published their findings on NetNut, an agent based out of the FBI's Houston office had been quietly looking into its operations, according to the documents and the people familiar with the investigation. The agent had been evaluating internet traffic records and

questioning people to try to determine how, if at all, NetNut was involved with the Popa software, according to the people and records.

There are multiple versions of Popa software. It wasn't clear if the FBI probe was focused on a specific variant.

In December, the agent's efforts were showcased during the gathering of law enforcement officials and industry experts just outside Denver, according to the people and records.

* * *

The investigations are primarily focused on a market that has formed out of selling and reselling packaged access to millions of devices on proxy networks for as little as a few dollars per gigabyte of data. Analysts have estimated that this market generates anywhere from $100 million to $3 billion in sales annually and that it will continue to grow in part because AI software developers have a voracious appetite for data scraped from websites.

"We've gone from a market in the tens of millions of dollars to the billions," Labovitz said. "This largely seems to be due to AI companies."

NetNut, which was acquired by what is now Alarum in 2019, presents itself as a major player in this market, offering tens of millions of proxy addresses in a system that ensures "complete anonymity and high speed."

In May, Alarum reported $11.7 million in first-quarter revenue, a 64% jump from the year earlier, saying "the growth was driven mainly by strong demand for the company's proxy solutions, as well as increased sales of new products."

49. On this news, the Company's share price fell $3.27 or 51.50%, to close at $3.08 on July 6, 2026, on unusually heavy trading volume.

CLASS ACTION ALLEGATIONS

50. 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 and entities that purchased or otherwise acquired Alarum securities between March 29, 2022 and July 2, 2026, inclusive, and who were damaged thereby (the "Class"). Excluded from the Class are Defendants, the officers and directors of the Company, at all relevant times, members of their immediate families and their

legal representatives, heirs, successors, or assigns, and any entity in which Defendants have or had a controlling interest.

51. The members of the Class are so numerous that joinder of all members is impracticable. Throughout the Class Period, Alarum's shares actively traded on the NASDAQ. While the exact number of Class members is unknown to Plaintiff at this time and can only be ascertained through appropriate discovery, Plaintiff believes that there are at least hundreds or thousands of members in the proposed Class. Millions of Alarum shares were traded publicly during the Class Period on the NASDAQ. Record owners and other members of the Class may be identified from records maintained by Alarum or its transfer agent and may be notified of the pendency of this action by mail, using the form of notice similar to that customarily used in securities class actions.

52. 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.

53. 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.

54. 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:

(a) whether the federal securities laws were violated by Defendants' acts as alleged herein;

(b) whether statements made by Defendants to the investing public during the Class Period omitted and/or misrepresented material facts about the business, operations, and prospects of Alarum; and

(c) to what extent the members of the Class have sustained damages and the proper measure of damages.

55. 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 makes 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.

UNDISCLOSED ADVERSE FACTS

56. The market for Alarum's securities was open, well-developed and efficient at all relevant times. As a result of these materially false and/or misleading statements, and/or failures to disclose, Alarum's securities traded at artificially inflated prices during the Class Period. Plaintiff and other members of the Class purchased or otherwise acquired Alarum's securities relying upon the integrity of the market price of the Company's securities and market information relating to Alarum, and have been damaged thereby.

57. During the Class Period, Defendants materially misled the investing public, thereby inflating the price of Alarum's securities, by publicly issuing false and/or misleading statements and/or omitting to disclose material facts necessary to make Defendants' statements, as set forth herein, not false and/or misleading. The statements and omissions were materially false and/or misleading because they failed to disclose material adverse information and/or misrepresented the truth about Alarum's business, operations, and prospects as alleged herein.

58. At all relevant times, the material misrepresentations and omissions particularized in this Complaint directly or proximately caused or were a substantial contributing cause of the damages sustained by Plaintiff and other members of the Class. As described herein, during the Class Period, Defendants made or caused to be made a series of materially false and/or misleading statements about Alarum's financial well-being and prospects. These material misstatements and/or omissions had the cause and effect of creating in the market an unrealistically positive assessment of the Company and its financial well-being and prospects, thus causing the Company's securities to be overvalued and artificially inflated at all relevant times. Defendants' materially false and/or misleading statements during the Class Period resulted in Plaintiff and other members of the Class purchasing the Company's securities at artificially inflated prices, thus causing the damages complained of herein when the truth was revealed.

LOSS CAUSATION

59. Defendants' wrongful conduct, as alleged herein, directly and proximately caused the economic loss suffered by Plaintiff and the Class.

60. During the Class Period, Plaintiff and the Class purchased Alarum's securities at artificially inflated prices and were damaged thereby. The price of the Company's securities significantly declined when the misrepresentations made to the market, and/or the information alleged herein to have been concealed from the market, and/or the effects thereof, were revealed, causing investors' losses.

SCIENTER ALLEGATIONS

61. As alleged herein, Defendants acted with scienter since Defendants knew that the public documents and statements issued or disseminated in the name of the Company were materially false and/or misleading; 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 federal securities laws. As set forth elsewhere herein in detail, the Individual Defendants, by virtue of their receipt of information reflecting the true facts regarding Alarum, their control over, and/or receipt and/or modification of Alarum's allegedly materially misleading misstatements and/or their associations with the Company which made them privy to confidential proprietary information concerning Alarum, participated in the fraudulent scheme alleged herein.

APPLICABILITY OF PRESUMPTION OF RELIANCE

(FRAUD-ON-THE-MARKET DOCTRINE)

62. The market for Alarum's securities was open, well-developed and efficient at all relevant times. As a result of the materially false and/or misleading statements and/or failures to disclose, Alarum's securities traded at artificially inflated prices during the Class Period. On July 3, 2024, the Company's share price closed at a Class Period high of $45.96 per share. Plaintiff and other members of the Class purchased or otherwise acquired the Company's securities relying upon the integrity of the market price of Alarum's securities and market information relating to Alarum, and have been damaged thereby.

63. During the Class Period, the artificial inflation of Alarum's shares was caused by the material misrepresentations and/or omissions particularized in this Complaint causing the damages sustained by Plaintiff and other members of the Class. As described herein, during the Class Period, Defendants made or caused to be made a series of materially false and/or misleading statements about Alarum's business, prospects, and operations. These material misstatements and/or omissions created an unrealistically positive assessment of Alarum and its business, operations, and prospects, thus causing the price of the Company's securities to be artificially inflated at all relevant times, and when disclosed, negatively affected the value of the Company shares. Defendants' materially false and/or misleading statements during the Class Period resulted

in Plaintiff and other members of the Class purchasing the Company's securities at such artificially inflated prices, and each of them has been damaged as a result.

64. At all relevant times, the market for Alarum's securities was an efficient market for the following reasons, among others:

(a) Alarum shares met the requirements for listing, and was listed and actively traded on the NASDAQ, a highly efficient and automated market;

(b) As a regulated issuer, Alarum filed periodic public reports with the SEC and/or the NASDAQ;

(c) Alarum regularly communicated with public investors via established market communication mechanisms, including through regular dissemination of press releases on the national circuits of major newswire services and through other wide-ranging public disclosures, such as communications with the financial press and other similar reporting services; and/or

(d) Alarum was followed by securities analysts employed by brokerage firms who wrote reports about the Company, and these reports were distributed to the sales force and certain customers of their respective brokerage firms. Each of these reports was publicly available and entered the public marketplace.

65. As a result of the foregoing, the market for Alarum's securities promptly digested current information regarding Alarum from all publicly available sources and reflected such information in Alarum's share price. Under these circumstances, all purchasers of Alarum's securities during the Class Period suffered similar injury through their purchase of Alarum's securities at artificially inflated prices and a presumption of reliance applies.

66. A Class-wide presumption of reliance is also appropriate in this action under the Supreme Court's holding in *Affiliated Ute Citizens of Utah v. United States*, 406 U.S. 128 (1972),

because the Class's claims are, in large part, grounded on Defendants' material misstatements and/or omissions. Because this action involves Defendants' failure to disclose material adverse information regarding the Company's business operations and financial prospects—information that Defendants were obligated to disclose—positive proof of reliance is not a prerequisite to recovery. All that is necessary is that the facts withheld be material in the sense that a reasonable investor might have considered them important in making investment decisions. Given the importance of the Class Period material misstatements and omissions set forth above, that requirement is satisfied here.

NO SAFE HARBOR

67. The statutory safe harbor provided for forward-looking statements under certain circumstances does not apply to any of the allegedly false statements pleaded in this Complaint. The statements alleged to be false and misleading herein all relate to then-existing facts and conditions. In addition, to the extent certain of the statements alleged to be false may be characterized as forward looking, they were not identified as "forward-looking statements" when made and there were no meaningful cautionary statements identifying important factors that could cause actual results to differ materially from those in the purportedly forward-looking statements. In the alternative, to the extent that the statutory safe harbor is determined to apply to any forward-looking statements pleaded herein, Defendants are liable for those false forward-looking statements because at the time each of those forward-looking statements was made, the speaker had actual knowledge that the forward-looking statement was materially false or misleading, and/or the forward-looking statement was authorized or approved by an executive officer of Alarum who knew that the statement was false when made.

FIRST CLAIM

Violation of Section 10(b) of The Exchange Act and

Rule 10b-5 Promulgated Thereunder

Against All Defendants

68. Plaintiff repeats and re-alleges each and every allegation contained above as if fully set forth herein.

69. During the Class Period, Defendants carried out a plan, scheme and course of conduct which was intended to and, throughout the Class Period, did: (i) deceive the investing public, including Plaintiff and other Class members, as alleged herein; and (ii) cause Plaintiff and other members of the Class to purchase Alarum's securities at artificially inflated prices. In furtherance of this unlawful scheme, plan and course of conduct, Defendants, and each defendant, took the actions set forth herein.

70. Defendants (i) employed devices, schemes, and artifices to defraud; (ii) made untrue statements of material fact and/or omitted to state material facts necessary to make the statements not misleading; and (iii) engaged in acts, practices, and a course of business which operated as a fraud and deceit upon the purchasers of the Company's securities in an effort to maintain artificially high market prices for Alarum's securities in violation of Section 10(b) of the Exchange Act and Rule 10b-5. All Defendants are sued either as primary participants in the wrongful and illegal conduct charged herein or as controlling persons as alleged below.

71. Defendants, individually and in concert, directly and indirectly, by the use, means or instrumentalities of interstate commerce and/or of the mails, engaged and participated in a continuous course of conduct to conceal adverse material information about Alarum's financial well-being and prospects, as specified herein.

72. Defendants employed devices, schemes and artifices to defraud, while in possession of material adverse non-public information and engaged in acts, practices, and a course of conduct as alleged herein in an effort to assure investors of Alarum's value and performance and continued substantial growth, which included the making of, or the participation in the making of, untrue statements of material facts and/or omitting to state material facts necessary in order to make the statements made about Alarum and its business operations and future prospects in light of the circumstances under which they were made, not misleading, as set forth more particularly herein, and engaged in transactions, practices and a course of business which operated as a fraud and deceit upon the purchasers of the Company's securities during the Class Period.

73. Each of the Individual Defendants' primary liability and controlling person liability arises from the following facts: (i) the Individual Defendants were high-level executives and/or directors at the Company during the Class Period and members of the Company's management team or had control thereof; (ii) each of these defendants, by virtue of their responsibilities and activities as a senior officer and/or director of the Company, was privy to and participated in the creation, development and reporting of the Company's internal budgets, plans, projections and/or reports; (iii) each of these defendants enjoyed significant personal contact and familiarity with the other defendants and was advised of, and had access to, other members of the Company's management team, internal reports and other data and information about the Company's finances, operations, and sales at all relevant times; and (iv) each of these defendants was aware of the Company's dissemination of information to the investing public which they knew and/or recklessly disregarded was materially false and misleading.

74. Defendants had actual knowledge of the misrepresentations and/or omissions of material facts set forth herein, or acted with reckless disregard for the truth in that they failed to

ascertain and to disclose such facts, even though such facts were available to them. Such defendants' material misrepresentations and/or omissions were done knowingly or recklessly and for the purpose and effect of concealing Alarum's financial well-being and prospects from the investing public and supporting the artificially inflated price of its securities. As demonstrated by Defendants' overstatements and/or misstatements of the Company's business, operations, financial well-being, and prospects throughout the Class Period, Defendants, if they did not have actual knowledge of the misrepresentations and/or omissions alleged, were reckless in failing to obtain such knowledge by deliberately refraining from taking those steps necessary to discover whether those statements were false or misleading.

75. As a result of the dissemination of the materially false and/or misleading information and/or failure to disclose material facts, as set forth above, the market price of Alarum's securities was artificially inflated during the Class Period. In ignorance of the fact that market prices of the Company's securities were artificially inflated, and relying directly or indirectly on the false and misleading statements made by Defendants, or upon the integrity of the market in which the securities trades, and/or in the absence of material adverse information that was known to or recklessly disregarded by Defendants, but not disclosed in public statements by Defendants during the Class Period, Plaintiff and the other members of the Class acquired Alarum's securities during the Class Period at artificially high prices and were damaged thereby.

76. At the time of said misrepresentations and/or omissions, Plaintiff and other members of the Class were ignorant of their falsity, and believed them to be true. Had Plaintiff and the other members of the Class and the marketplace known the truth regarding the problems that Alarum was experiencing, which were not disclosed by Defendants, Plaintiff and other members of the Class would not have purchased or otherwise acquired their Alarum securities, or, if they

had acquired such securities during the Class Period, they would not have done so at the artificially inflated prices which they paid.

77. By virtue of the foregoing, Defendants violated Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder.

78. As a direct and proximate result of Defendants' wrongful conduct, Plaintiff and the other members of the Class suffered damages in connection with their respective purchases and sales of the Company's securities during the Class Period.

SECOND CLAIM

Violation of Section 20(a) of The Exchange Act

Against the Individual Defendants

79. Plaintiff repeats and re-alleges each and every allegation contained above as if fully set forth herein.

80. Individual Defendants acted as controlling persons of Alarum within the meaning of Section 20(a) of the Exchange Act as alleged herein. By virtue of their high-level positions and their ownership and contractual rights, participation in, and/or awareness of the Company's operations and intimate knowledge of the false financial statements filed by the Company with the SEC and disseminated to the investing public, Individual Defendants had the power to influence and control and did influence and control, directly or indirectly, the decision-making of the Company, including the content and dissemination of the various statements which Plaintiff contends are false and misleading. Individual Defendants were provided with or had unlimited access to copies of the Company's reports, press releases, public filings, and other statements alleged by Plaintiff to be misleading prior to and/or shortly after these statements were issued and had the ability to prevent the issuance of the statements or cause the statements to be corrected.

81. In particular, Individual Defendants had direct and supervisory involvement in the day-to-day operations of the Company and, therefore, had the power to control or influence the particular transactions giving rise to the securities violations as alleged herein, and exercised the same.

82. As set forth above, Alarum and Individual Defendants each violated Section 10(b) and Rule 10b-5 by their acts and omissions as alleged in this Complaint. By virtue of their position as controlling persons, Individual Defendants are liable pursuant to Section 20(a) of the Exchange Act. As a direct and proximate result of Defendants' wrongful conduct, Plaintiff and other members of the Class suffered damages in connection with their purchases of the Company's securities during the Class Period.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief and judgment, as follows:

(a) Determining that this action is a proper class action under Rule 23 of the Federal Rules of Civil Procedure;

(b) Awarding compensatory damages in favor of Plaintiff and the other Class members against all defendants, jointly and severally, for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

(c) Awarding Plaintiff and the Class their reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

(d) Such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury.

Dated: July ___, 2026

GLANCY PRONGAY WOLKE & ROTTER LLP

By: _____
Rebecca Dawson
745 5th Avenue, 5th Floor
New York, NY 10151
Telephone: (213) 521-8007
Facsimile: (212) 884-0988
Email: rdawson@glancylaw.com

Robert V. Prongay
Charles H. Linehan
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Telephone: (310) 201-9150
Facsimile: (310) 201-9160
clinehan@glancylaw.com

LAW OFFICES OF HOWARD G. SMITH
Howard G. Smith
3070 Bristol Pike, Suite 112
Bensalem PA 19020
Telephone: (215) 638-4847
Facsimile: (215) 638-4867

Counsel for Plaintiff _____