Vanguard

P.O. Box 2600
Valley Forge, PA 19482

vanguard.com

August 4, 2025

Electronic Delivery VIA EDGAR
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Re: Amended Filing Pursuant to Section 33 of the Investment Company Act of 1940: Brian Felsen, Matthew Ragusano, and Nambaramey Dy, Individually and on behalf of all others similarly situated v. The Vanguard Group, Inc.; Case No. 2:25-cv-02359 (United States District Court for the Eastern District of Pennsylvania)

Dear Sir or Madam,

Enclosed for filing on behalf of The Vanguard Group, Inc., pursuant to Section 33 of the Investment Company Act of 1940, is a copy of the amended complaint filed by Brian Felsen, Matthew Ragusano, and Nambaramey Dy, individually and on behalf of all others similarly situated.

If you have any questions regarding this filing, please contact me at (610) 503-3877.

Please acknowledge receipt by sending a confirmation email to Fund_&_Advisor_Regulatory_Engagements@vanguard.com.

Sincerely,

Signed by:
Jacqueline Angell
493E33E30629494...

8/5/2025 | 11:23 AM EDT

Jacqueline Mary Angell
Chief Compliance Officer
The Vanguard Group, Inc.

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

BRIAN FELSEN, MATTHEW RAGUSANO, and NAMBARAMEY DY, individually and on behalf of all others situated, Plaintiffs, v. THE VANGUARD GROUP, INC., Defendant.	Case No. 2:25-cv-02359-JFM **FIRST AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Brian Felsen, Matthew Ragusano, and Nambaramey Dy ("Plaintiffs") bring this action on behalf of themselves and all others similarly situated against Defendant The Vanguard Group, Inc. ("Defendant" or "Vanguard"). Plaintiffs bring this action based on personal knowledge of the facts pertaining to themselves, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

NATURE OF THE ACTION

1. This lawsuit is bought on behalf of all Vanguard accountholders who accessed their accounts on investor.vanguard.com (the "Website") and on Vanguard's mobile application (the "App") due to Defendant's practice of surreptitiously disclosing sensitive and confidential financial information of its accountholder to third parties.

2. The Website and the App are owned and operated by Defendant. Defendant operates an investment service through which consumers can manage brokerage, educational savings, or personal or workplace retirement accounts. To create an account, consumers must share personally identifying information, including their name and email address. Consumers can then purchase stocks and other investment products through their account. When users disclose

such sensitive information to access these services, data privacy is paramount to maintaining consumer trust. On the account creation pages, Vanguard represents that "[t]his application is secure." Indeed, users would not disclose such information if they suspected that it was not being safeguarded.

3. Nonetheless, and unbeknownst to Plaintiffs and members of the putative class, Defendant discloses and assists several third parties, including LinkedIn Corporation ("LinkedIn"), Google LLC ("Google"), and Meta Platforms, Inc. ("Meta") (each, a "Third Party" and collectively, the "Third Parties") in intentionally intercepting these sensitive and confidential communications. The Third Parties then match the information they receive from Defendant to the specific Third Party profile of the user who provided the information.

4. Neither Defendant nor the Third Parties received consent for these interceptions, thereby engaging in conduct that expressly contravenes their own terms and representations.

5. Despite reasonable expectations of privacy and Defendant's legal duties to prevent the disclosure of such private information, Defendant disclosed and assisted the Third Parties in intentionally intercepting confidential information from Defendant's Website and App for target advertising purposes and to increase their own revenue. These disclosures include communications that contain sensitive and confidential information – i.e., "nonpublic personal information," as defined by 16 C.F.R. § 313.3 (the "Gramm-Leach-Bliley Act" or "GLBA") and Cal. Fin. Code § 4050, et seq. (the "California Financial Information Privacy Act" or "CalFIPA"). Plaintiffs bring this action for legal and equitable remedies resulting from these illegal acts.

PARTIES

6. Plaintiff Brian Felsen ("Plaintiff Felsen") is a natural person domiciled in Los Angeles, California. Plaintiff Felsen has held an investment account with Defendant since 1991. Plaintiff Felsen regularly logs into his account and searches for and purchases investments on the Website while in California, including as recently as April 2025.[1] Plaintiff Felsen also maintained LinkedIn and Facebook accounts at all relevant times.

7. Plaintiff Matthew Ragusano ("Plaintiff Ragusano") is a natural person domiciled in Los Angeles, California. Plaintiff Ragusano has held an account with Defendant since 2012. Plaintiff Ragusano regularly logs into his account and searches for and purchases investments on the App while in California, including as recently as April 2025. Plaintiff Ragusano also maintained a LinkedIn account at all relevant times.

8. Plaintiff Nambaramey Dy ("Plaintiff Dy") is a natural person domiciled in Norwood, Pennsylvania. Plaintiff Dy has held an investment account with Defendant since 2018. Plaintiff Felsen regularly logs into his account and searches for and purchases investments on the Website and App while in Pennsylvania, including as recently as June 2025. Plaintiff Dy also maintained a LinkedIn account at all relevant times.

9. Defendant The Vanguard Group, Inc. is a Delaware Corporation with its principal place of business in Valley Forge, Pennsylvania. At all times, Defendant knew that the incorporation of the Third Party tracking technologies onto its Website and App would result in the interception of confidential financial and personal information. Defendant, as the operator of its Website and App, knew that its users' interactions on the Website and App were being intercepted in real time. Defendant is well aware of the dangers of incorporating such

[1] The specific trades executed by the Plaintiffs are omitted to protect their privacy.

technology onto its Website and App, which collects such sensitive information, but continues to do so due to the value of the data that is intercepted.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this class action because it arises under a law of the United States, namely, 18 U.S.C. § 2511(1). This Court also has supplemental jurisdiction over Plaintiff's state law claims under 28 U.S.C. §1367. Further, this action is a putative class action, and Plaintiff alleges that at least one member of the Classes, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs.

11. This Court has personal jurisdiction over the parties because Defendant's principal place of business is in Pennsylvania, Plaintiff submits to the jurisdiction of the Court, and because Defendant, at all times relevant hereto, has systematically and continually conducted business in Pennsylvania.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant includes a choice of law provision and choice of venue provision in its Website and App selecting Pennsylvania law and the United States District Court for the Eastern District of Pennsylvania, respectively. Defendant, therefore, consents to venue in this Court.

FACTUAL ALLEGATIONS

13. Vanguard is an investment services company that connects consumers to securities and similar financial products. Defendant's Website, investor.vanguard.com (the "Website"), and mobile application (the "App") are at issue in this action.

14. Vanguard purports to "empower[] investors"[2] and to provide "products to support your financial strategy."[3]

15. On their accounts, users must provide Vanguard with personal information to purchase individual investments, including, but not limited to, their name, email, date of birth, social security number, citizenship status, gender, residential address, and phone number. Unbeknownst to users, multiple third-party companies were tracking their activity from the moment they entered the Vanguard Website or App.

16. Investors then add money to their investment accounts and use that money to purchase investments by searching for and selecting the investment products they wish to purchase.

I. THE GRAMM-LEACH-BLILEY ACT AND CALIFORNIA FINANCIAL INFORMATION PRIVACY ACT

17. As Congress and the California Legislature recognized, "nonpublic personal information" is confidential.

18. Per 16 C.F.R. § 313.3(n):

> (1) Nonpublic personal information means:
>
> (i) Personally identifiable financial information; and
>
> (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

19. Per 16 C.F.R. § 313.3(o):

> (1) Personally identifiable financial information means any information:
>
> (i) A consumer provides to [a financial institution] to obtain a financial product or service from [a financial institution];

[2] VANGUARD, HOMEPAGE, *available at* https://investor.vanguard.com
[3] *Id.*

(ii) About a consumer resulting from any transaction involving a financial product or service between [a financial institution] and a consumer; or

(iii) [A financial institution] otherwise obtain[s] about a consumer in connection with providing a financial product or service to that consumer.

(2) Examples—(i) Information included. Personally identifiable financial information includes:

(A) Information a consumer provides to [a financial institution]on an application to obtain a loan, credit card, or other financial product or service;

(B) Account balance information, payment history, overdraft history, and credit or debit card purchase information;

(C) The fact that an individual is or has been one of [a financial institution's] customers or has obtained a financial product or service from [a financial institution];

(D) Any information about [a financial institution's] consumer if it is disclosed in a manner that indicates that the individual is or has been [a financial institution's] consumer;

(E) Any information that a consumer provides to [a financial institution] or that [a financial institution]or [its] agent otherwise obtain[s] in connection with collecting on, or servicing, a credit account; and

(F) Any information [a financial institution] collect[s] through an Internet "cookie" (an information collecting device from a web server).

20. Pursuant to 16 C.F.R. § 313.3(k)(1), Defendant is a financial institution.

21. In passing CalFIPA, the California Legislature "intend[ed] for financial institutions to provide their consumers notice and meaningful choice about how consumers' nonpublic personal information is shared or sold by their financial institutions[]" and "inten[ded] . . . to afford persons greater privacy protections than those provided in Public Law 106-102, the federal Gramm-Leach-Bliley Act[.]" Cal. Fin. Code § 4051(a)-(b).

22. Cal. Fin. Code § 4052(a) provides:

> "Nonpublic personal information" means personally identifiable financial information (1) provided by a consumer to a financial institution, (2) resulting from any transaction with the consumer or any service performed for the consumer, or (3) otherwise obtained by the financial institution. Nonpublic personal information does not include publicly available information that the financial institution has a reasonable basis to believe is lawfully made available to the general public from (1) federal, state, or local government records, (2) widely distributed media, or (3) disclosures to the general public that are required to be made by federal, state, or local law. Nonpublic personal information shall include any list, description, or other grouping of consumers, and publicly available information pertaining to them, that is derived using any nonpublic personal information other than publicly available information, but shall not include any list, description, or other grouping of consumers, and publicly available information pertaining to them, that is derived without using any nonpublic personal information.

23. According to Cal. Fin. Code § 4052(b):

> "Personally identifiable financial information" means information (1) that a consumer provides to a financial institution to obtain a product or service from the financial institution, (2) about a consumer resulting from any transaction involving a product or service between the financial institution and a consumer, or (3) that the financial institution otherwise obtains about a consumer in connection with providing a product or service to that consumer. Any personally identifiable information is financial if it was obtained by a financial institution in connection with providing a financial product or service to a consumer. Personally identifiable financial information includes all of the following:
>
> (1) Information a consumer provides to a financial institution on an application to obtain a loan, credit card, or other financial product or service.
>
> (2) Account balance information, payment history, overdraft history, and credit or debit card purchase information.
>
> (3) The fact that an individual is or has been a consumer of a financial institution or has obtained a financial product or service from a financial institution.
>
> (4) Any information about a financial institution's consumer if it is disclosed in a manner that indicates that the individual is or has been the financial institution's consumer.

> (5) Any information that a consumer provides to a financial institution or that a financial institution or its agent otherwise obtains in connection with collecting on a loan or servicing a loan.
>
> (6) Any personally identifiable financial information collected through an Internet cookie or an information collecting device from a Web server.

24. "Except as provided in Sections 4053, 4054.6, and 4056, a financial institution shall not sell, share, transfer, or otherwise disclose nonpublic personal information to or with any nonaffiliated third parties without the explicit prior consent of the consumer to whom the nonpublic personal information relates." Cal. Fin. Code § 4052.5.

25. Thus, Plaintiffs' and Class Members' "nonpublic personal information" is confidential under both federal and California law. Nonetheless, such information was intercepted in transit by each Third Party—as enabled by Defendant—and neither Defendant nor the Third Parties procured Plaintiffs' and Class Members' consent prior to this interception.

26. This pattern of conduct by Defendant flouts the GLBA's and CalFIPA's respective purposes of enhancing "financial privacy[.]"[4]

II. OVERVIEW OF THE THIRD PARTY TRACKING TECHNOLOGIES

A. The LinkedIn Insight Tag

27. LinkedIn markets itself as "the world's largest professional network on the internet[.]"[5] But LinkedIn is no longer simply a tool to help its users find jobs or expand their professional network. LinkedIn has moved into the marketing and advertising space and boasts of its ability to allow potential advertisers to "[r]each 1 billion+ professionals around the world"

[4] http://www.leginfo.ca.gov/pub/03-04/statute/ch_0201-0250/ch_241_st_2003_sb_1. *See also* https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=200320040SB1.
[5] LINKEDIN, WHAT IS LINKEDIN AND HOW CAN I USE IT?, https://www.linkedin.com/help/linkedin/answer/a548441#.

via its Marketing Solutions services.[6] Recently, LinkedIn was projected as being responsible for "roughly 0.9 percent of the global ad revenue" which included approximately $5.91 billion in advertising revenue in 2022.[7]

28. According to LinkedIn, "[t]argeting is a foundational element of running a successful advertising campaign — [g]etting your targeting right leads to higher engagement, and ultimately, higher conversion rates." [8] Targeting refers to ensuring that advertisements are tailored to, and appear in front of, the intended demographic for an advertisement. To that end, LinkedIn's Marketing Solutions services allow potential advertisers to "[b]uild strategic campaigns" targeting specific users.[9] LinkedIn's "marketing solutions allow advertisers to select specific characteristics to help them reach their ideal audience. The ads [users] see on LinkedIn are then targeted to provide content relevant to [the users]."[10]

29. As a result of its activities and operation of the LinkedIn Insight Tag, LinkedIn can make extremely personal inferences about individuals' demographics, intent, behavior, engagement, interests, buying decisions, and more.[11]

---

[6] LINKEDIN, MARKETING SOLUTIONS, https://business.linkedin.com/marketing-solutions.
[7] Valentina Dencheva, *LinkedIn annual ad revenue 2017-2027*, STATISTA (Dec. 12, 2023), https://www.statista.com/statistics/275933/linkedins-advertising-revenue.
[8] LINKEDIN, REACH YOUR AUDIENCE: TARGETING ON LINKEDIN, p.3, https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/resources/pdfs/linkedin-targeting-playbook-v3.pdf.
[9] LINKEDIN, *supra* note 4.
[10] LINKEDIN, LINKEDIN ADS AND MARKETING SOLUTIONS, https://www.linkedin.com/help/lms/answer/a421454.
[11] *See* LINKEDIN, MARKETING SOLUTIONS, https://business.linkedin.com/marketing-solutions/audience ("Target audiences through demographic marketing[,]" "Zero in on intent, behavior, engagement, interests, and more[,]" and "Reach the LinkedIn audience involved in the buying decision").

30. The personal information and communications obtained by LinkedIn are used to fuel various services offered via LinkedIn's Marketing Solutions including Ad Targeting, Matched Audiences, Audience Expansion, and LinkedIn Audience Network.[12]

31. Such information is extremely valuable to marketers and advertisers because the inferences derived from users' personal information and communications allow marketers and advertisers to target potential customers.[13]

32. For example, through the use of LinkedIn's Audience Network, marketers and advertisers are able to expand their reach and advertise on sites other than LinkedIn to "reach millions of professionals across multiple touchpoints."[14] According to Broc Munro of Microsoft, which owns LinkedIn, "[w]e gravitate towards social platforms like LinkedIn to achieve more targeted marketing engagement. However, we know that our audiences don't spend all their time on social media. LinkedIn Audience Network enables us to expand our reach to trusted sites while still respecting our audience targeting. This increases the impact of our advertising."[15]

---

[12] *See id.*

[13] LINKEDIN, PRIVACY POLICY, https://www.linkedin.com/legal/privacy-policy ("We serve you tailored ads both on and off our Services. We offer you choices regarding personalized ads, but you cannot opt-out of seeing other ads."); LINKEDIN, ACCOUNT TARGETING, https://business.linkedin.com/marketing-solutions/ad-targeting ("Target your ideal customer based on traits like their job title, company name or industry, and by professional or personal interests"); LINKEDIN, EXAMPLES OF TRENDING AND BEST-IN-CLASS HEALTHCARE CAMPAIGNS AND CONTENT, p.6, https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/healthcare-microsite/resources/lkin-lms-sales-healthcare-campaigns-trending-content-Jan2023.pdf ("BD zeroed in on the end-benefit with a 30 second video introducing their PIVO needle-free blood collection device to potential customers."); LINKEDIN, HEALTHCARE SOCIAL MEDIA STRATEGIES FOR 2023, p.1, https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/healthcare-microsite/resources/hc-social-media-trends.pdf (listing "potential customers" as "Common audiences" for insurance sector).

[14] LINKEDIN, ACCOUNT TARGETING, https://business.linkedin.com/marketing-solutions/ad-targeting.

[15] LINKEDIN, LINKEDIN AUDIENCE NETWORK, https://business.linkedin.com/marketing-solutions/native-advertising/linkedin-audience-network.

33. In July 2022, "LinkedIn Marketing Solutions surpassed $5 billion in annual revenue[.]"[16] That figure is "expected to further grow to reach 10.35 billion U.S. dollars by 2027."[17]

34. According to LinkedIn, the LinkedIn Insight Tag is "[a] simple code snippet added to [a] website [that] can help you optimize your campaigns, retarget your website visitors, and learn more about your audiences."[18] LinkedIn represents that the LinkedIn Insight Tag "enable[s] in-depth campaign reporting and unlock[s] valuable insights about your website visitors."[19]

35. LinkedIn's current iteration of its Insight Tag is a JavaScript-based code which allows for the installation of its software.[20] A critical feature allows the LinkedIn Insight Tag to track users, even when third-party cookies are blocked.[21] LinkedIn "recommend[s] using the JavaScript-based Insight Tag or Conversions API" because third-party cookie settings are being deprecated across the industry.[22] Embedding the JavaScript as a first-party cookie causes users' browsers to treat the LinkedIn Insight Tag as though it is offered by the website being visited, rather than by third-party LinkedIn. Doing so ensures that the third-party cookie-blocking

---

[16] *LinkedIn Business Highlights from Microsoft's FY22 Q4 Earnings*, LINKEDIN PRESSROOM (July 25, 2022), https://news.linkedin.com/2022/july/linkedin-business-highlights-from-microsoft-s-fy22-q4earnings#:~:text=And%20LinkedIn%20Marketing%20Solutions%20surpassed,revenue%20for%20the%20first%20time.

[17] Dencheva, *supra* note 5.

[18] LINKEDIN, INSIGHT TAG, https://business.linkedin.com/marketing-solutions/insight-tag.

[19] LINKEDIN, LINKEDIN INSIGHT TAG FAQS, https://www.linkedin.com/help/lms/answer/a427660.

[20] LINKEDIN, *supra* note 16.

[21] *Id.* ("It's important for advertisers to prepare for these changes by switching to JavaScript tags and enabling 'enhanced conversion tracking' in the Insight Tag settings to continue capturing signals where 3rd party cookies are blocked.").

[22] *See id.*

functions of modern web browsers do not prevent LinkedIn from collecting data through its software.[23] Instead, the LinkedIn Insight Tag is shielded with the same privacy exemptions offered to first-party cookies.

36. When a user who has signed in to LinkedIn (even if the user has subsequently logged out) is browsing a website where the LinkedIn Insight Tag has been embedded, an HTTP request is sent using cookies, which includes information about the user's actions on the website.

37. These cookies also include data that differentiates users from one another and can be used to link the data collected to the user's LinkedIn profile.

38. The HTTP request about an individual who has previously signed into LinkedIn includes requests from the "li_sugr" and "lms_ads" cookies. Each of these cookies are used by LinkedIn "to identify LinkedIn Members off LinkedIn" for advertising purposes.[24]

39. For example, the "li_sugr" cookie is "[u]sed to make a probabilistic match of a user's identity."[25] Similarly, the "lms_ads" cookie is "[u]sed to identify LinkedIn Members off LinkedIn for advertising."[26]

40. A LinkedIn profile contains information including an individual's first and last name, place of work, contact information, and other personal details. Based on information it obtains through the LinkedIn Insight Tag, LinkedIn is able to target its account holders for advertising.

[23] *See id.*
[24] LINKEDIN, LINKEDIN COOKIE TABLE, https://www.linkedin.com/legal/l/cookie-table.
[25] *See id.*
[26] *See id.*

41. LinkedIn never receives consent from users to intercept and collect electronic communications containing their sensitive and unlawfully disclosed information. In fact, LinkedIn expressly warrants the opposite.

42. When first signing up, a user agrees to the User Agreement.[27] By using or continuing to use LinkedIn's Services, users agree to two additional agreements: the Privacy Policy[28] and the Cookie Policy.[29] For California residents, LinkedIn also publishes a California Privacy Disclosure.[30]

43. LinkedIn's Privacy Policy begins by stating that "LinkedIn's mission is to connect the world's professionals . . . . Central to this mission is our commitment to be transparent about the data we collect about you, how it is used and with whom it is shared."[31]

44. The Privacy Policy goes on to describe what data LinkedIn collects from various sources, including cookies and similar technologies.[32] LinkedIn states "we use cookies and similar technologies (e.g., pixels and ad tags) to collect data (e.g., device IDs) to recognize you and your device(s) on, off and across different services and devices where you have engaged with our Services. We also allow some others to use cookies as described in our Cookie Policy."[33]

45. However, LinkedIn offers an express representation: "We will only collect and process personal data about you where we have lawful bases."[34]

---

[27] LINKEDIN, USER AGREEMENT, https://www.linkedin.com/legal/user-agreement.
[28] LINKEDIN, PRIVACY POLICY, https://www.linkedin.com/legal/privacy-policy.
[29] LINKEDIN, COOKIE POLICY, https://www.linkedin.com/legal/cookie-policy.
[30] LINKEDIN, CALIFORNIA PRIVACY DISCLOSURE, https://www.linkedin.com/legal/california-privacy-disclosure.
[31] LINKEDIN, PRIVACY POLICY, https://www.linkedin.com/legal/privacy-policy.
[32] *Id.*
[33] *Id.*
[34] *Id.*

46. Despite this explicit representation, LinkedIn intentionally intercepts and receives sensitive information in violation of state and federal privacy laws due to the value of the data.

47. Users never choose to provide sensitive information to LinkedIn because, among other reasons, they never know whether a particular website uses the LinkedIn Insight Tag, and, if so, what sensitive personal data it collects.

48. The LinkedIn Insight Tag was embedded on the Website and App, which allowed LinkedIn to intercept and record "click" events. Click events detail information from the Website and App including personal information from account creation, the type of account opened, queries in the search box, ticker symbol, and action taken along with an identifier used to track the visitor's identity across websites.

49. These interceptions also included the li_sugr and lms_ads cookies, which LinkedIn utilizes to identify its account holders for targeted advertising.

50. LinkedIn incorporated the information it intercepted from the Vanguard Website and App into its marketing tools to fuel its targeted advertising service.

51. The requested information is protected by state and federal law, and users would not disclose such information if they knew it was being unlawfully intercepted by a third party. Plaintiffs never consented, agreed, authorized, or otherwise permitted LinkedIn to intercept their confidential personal and financial information.

52. By law, Plaintiffs are entitled to privacy in their protected personal and financial information and confidential communications. Vanguard deprived Plaintiffs of their privacy rights when it implemented a system that surreptitiously tracked, recorded, and transmitted Plaintiffs' and other online users' confidential communications, personally identifiable information, and sensitive financial information.

53. One of LinkedIn's partners is Vanguard. The LinkedIn Insight Tag is employed on the Website and App in the manner described throughout this Complaint.

B. The Google Analytics Tracking Code

54. The Google Analytics tracking code is a piece of code that can be installed onto websites to track page visits, button clicks, text entered into websites, and other actions taken by website visitors, including information such as "how many users bought an item … by tracking whether they made it to the purchase-confirmation page."[35] The tracking code is connected to the Google Analytics platform.

55. According to Google, "Google Analytics is a platform that collects data from [] websites and apps to create reports that provide insights" for businesses.[36]

56. Google advertises that this service can "[m]onitor activity on your site as it happens."[37]

57. Google's business model involves entering into voluntary partnerships with various companies and surveilling communications on their partners' websites with the Google Analytics tracking code.

58. Thus, through websites that employ Google's services, Google directly receives the electronic communications that website visitors entered into search bars, chat boxes, and online questionnaires in real time.

59. When the Google Analytics tracking code is used on an entry to a website, it is not like a tape recorder or a "tool" used by one party to record the other. Instead, the Google

[35] "How Google Analytics Works" https://support.google.com/analytics/answer/12159447?hl=en&ref_topic=14089939&sjid=2827624563183915220-NC
[36] *Id*.
[37] "The Finer Points" https://marketingplatform.google.com/about/analytics/features/

Analytics tracking code involves Google, a separate and distinct third-party entity from the parties in the conversation, using the Google Analytics tracking code to eavesdrop on, record, extract information from, and analyze a conversation to which it is not a party. This is so because Google itself is collecting the content of any conversation. That information is then analyzed by Google before being provided to any entity that was a party to the conversation (like Defendant).

60. Once Google intercepts a website's communications, it has the capability to use such information for its own purposes. "Google uses the information shared by sites and apps to deliver [] services, maintain and improve them, develop new services, measure the effectiveness of advertising, protect against fraud and abuse, and personalize content and ads you see on Google and on [] partners' sites and apps."[38]

61. Google's range of SaaS services is based on Google's ability to collect and analyze information about users' web behavior and deliver targeted advertising to select consumers based on their web habits. This involves collecting visitor information from thousands of websites and then analyzing that information to deliver targeted advertising and group web users so that they can be targeted for products and categories they are interested in.

62. In sum, Google has the capability to use website communications to (i) improve its own products and services; (ii) develop new Google for Business and Google Analytics products and services; and (iii) analyze website visitors' communications to assist with data analytics and targeted advertising.

63. Information from websites and applications like Defendant's is central to Google's ability to successfully market their advertising capabilities to future clients.

[38] "Google Privacy and Terms," https://policies.google.com/technologies/partner-sites

64. On each page of Defendant's Website and App on which the Google tracking code is installed, Google Analytics collects the visitor's queries in the search box, ticker symbol of funds purchased, and other actions taken along with unique identifiers used to track the visitor's activity across websites, the language spoken on the site, and the visitor's browser, operating system, and Wi-Fi provider.

65. One of Google's partners is Vanguard. The Google Analytics tracking code is employed on the Website and App in the manner described throughout this Complaint.

C. The Meta Pixel

66. Facebook, owned by Meta, describes itself as a "real identity platform,"[39] meaning users are allowed only one account and must share "the name they go by in everyday life."[40] To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.[41]

67. Meta sells advertising space by highlighting its ability to target users.[42] Meta can target users so effectively because it surveils user activity both on and off its sites.[43] This allows Meta to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[44] Meta compiles this information into a generalized dataset

[39] Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).
[40] FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity.
[41] FACEBOOK, SIGN UP, https://www.facebook.com.
[42] FACEBOOK, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES, https://www.facebook.com/business/help/205029060038706.
[43] FACEBOOK, ABOUT META PIXEL, https://www.facebook.com/business/help/742478679120153?id=120537668283214.
[44] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.

called "Core Audiences," which allows advertisers to reach precise audiences based on specified targeting types.[45]

68. Advertisers can also build "Custom Audiences."[46] Custom Audiences enables advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[47] With Custom Audiences, advertisers can target existing customers directly, and they can also build "Lookalike Audiences," which "leverage[] information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[48] Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Meta with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers or by utilizing Meta's "Business Tools."[49]

69. As Meta puts it, the Business Tools "help website owners and publishers, app developers, and business partners, including advertisers and others, integrate with [Facebook], understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[50] Put more succinctly, Meta's Business

[45] https://www.facebook.com/business/news/Core-Audiences.
[46] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=246909795337649.
[47] FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.
[48] FACEBOOK, ABOUT LOOKALIKE AUDIENCES, https://www.facebook.com/business/help/164749007013531?id=401668390442328.
[49] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; FACEBOOK, CREATE A WEBSITE CUSTOM AUDIENCE, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494.
[50] FACEBOOK, THE META BUSINESS TOOLS, https://www.facebook.com/help/331509497253087.

Tools are bits of code that advertisers can integrate into their websites, mobile applications, and servers, thereby enabling Meta to intercept and collect user activity on those platforms.

70. The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[51] Meta's Business Tools can also track other events. Meta offers a menu of "standard events" from which advertisers can choose, including what content a visitor views or purchases.[52] Advertisers can even create their own tracking parameters by building a "custom event."[53]

71. One such Business Tool is the Meta Pixel (the "Meta Pixel"). Meta offers this piece of code to advertisers, like Defendant, to integrate into their websites. The Meta Pixel "tracks the people and type of actions they take."[54] When a user accesses a website hosting the Meta Pixel, Meta's software script surreptitiously directs the user's browser to contemporaneously send a separate message to Meta's servers. This secret and contemporaneous transmission contains the original GET request sent to the host website, along with additional data that the Meta Pixel is configured to collect. This transmission is initiated by Meta code and concurrent with the communications with the host website. At relevant times,

---

[51] *See* FACEBOOK, META FOR DEVELOPERS: META PIXEL, ADVANCED, https://developers.facebook.com/docs/meta-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR META PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, META FOR DEVELOPERS: MARKETING API - APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[52] FACEBOOK, SPECIFICATIONS FOR META PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142.

[53] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, META FOR DEVELOPERS: MARKETING API – APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[54] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting.

two sets of code were thus automatically run as part of the browser's attempt to load and read Defendant's Website and App—Defendant's own code and Facebook's embedded code.

72. Each time Defendant sent this activity data, it also disclosed a consumer's personally identifiable information, including their Facebook ID ("FID"). An FID is a unique and persistent identifier that Facebook assigns to each user. With it, any ordinary person can look up the user's Facebook profile and name. Notably, while Meta can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of an FID. Meta admits as much on its website. Indeed, ordinary persons who come into possession of the FID can connect to any Facebook profile.

73. A user who accessed Defendant's Website or App while logged into Facebook transmitted what is known as a "c_user cookie" to Facebook, which contained that user's unencrypted Facebook ID.

74. What is more, when a user checks out on the Website or App, Meta is sent the email address used to check out. The email address is encrypted by way of a process known as SHA256, which is a way to "hash" written words in a series of random numbers.

75. The Meta Pixel is designed to collect information about website visitors that can be matched to an individual's Facebook profile for the purpose of sending targeted advertising to that user. Though the "hashing" would prevent a party that is not Meta from obtaining the subscriber's email address, Meta, as the recipient of the data and the entity that creates the hash, can decrypt the hashed email addresses it receives and match it to the profile of Facebook users.

76. When the Meta Pixel is used on a website, it is not like a tape recorder or a "tool" used by one party to record the other. Instead, the Meta Pixel involves Meta, a separate and distinct third-party entity from the parties in the conversation, using the Meta Pixel to eavesdrop

on, record, extract information from, and analyze a conversation to which it is not a party. This is so because Meta itself is collecting the content of any conversation. That information is then analyzed by Meta before being provided to any entity that was a party to the conversation (like Defendant).

77. Once Meta intercepts website communications, it has the capability to use such information for its own purposes. In 2021, Meta generated over $117 billion in revenue.[55] With respect to the apps offered by Meta, substantially all of Meta's revenue is generated by selling advertising space.[56] Meta sells advertising space by highlighting its ability to target users by including them in the Core Audiences and Custom Audiences offered to its clients.[57]

78. In practice, this means the information collected is used to (i) analyze trends in consumer behavior based on data collected from websites across the internet that Meta can then use when providing targeted advertising to other companies, (ii) create consumer profiles of specific users, allowing Meta to sell future customers targeted advertising to consumers with specific profile characteristics, and (iii) develop new Meta Business Tools products and services, or improve pre-existing Meta Business Tools products and services.

79. One of Meta's partners is Vanguard. The Meta Pixel is employed on the Website and App in the manner described throughout this Complaint.

---

[55] FACEBOOK, META ANNUAL REPORT 2021, https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/2023/2021-Annual-Report.pdf at 51.
[56] *Id.* at 63.
[57] FACEBOOK, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES, https://www.facebook.com/business/help/205029060038706.

II. DEFENDANT INSTALLED THIRD PARTY TRACKING TECHNOLOGIES ON ITS WEBSITE AND APP

80. Defendant employed the services of the Third Parties and their tracking technologies on each page of its Website and App to track its users' investment activities and send this information to the Third Parties so the Third Parties could analyze the information and target users with advertising based on those activities.

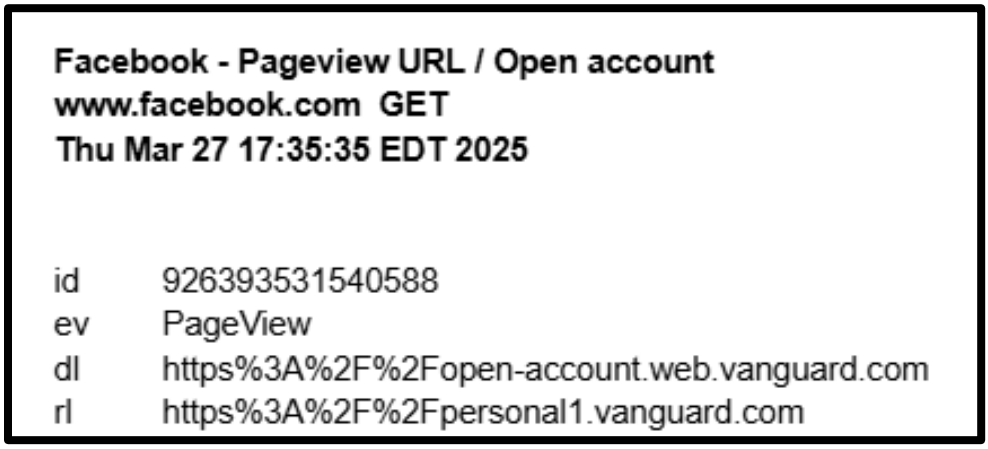
81. The images herein depict the series of screens shown to Website visitors when they navigate to the Website. The tracking technologies are installed on each page of the Website, collecting information from users who communicate with Defendant through the Website.

82. Defendant intercepted its users' confidential information from its Website to monetize that data through targeted advertising.

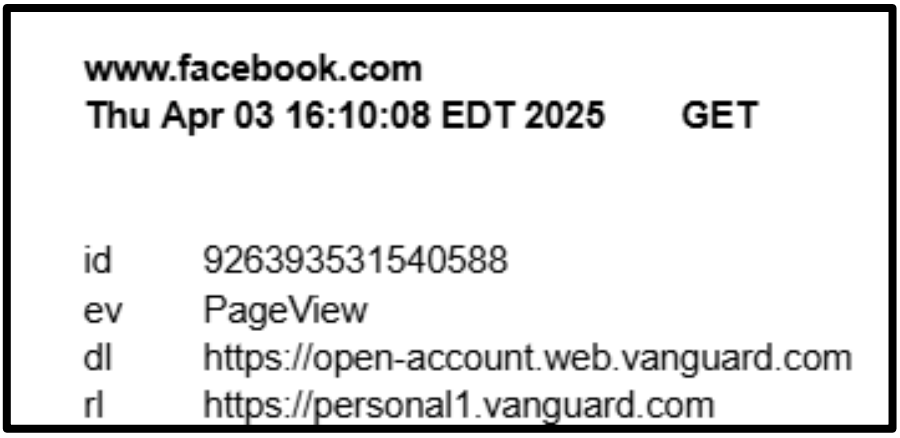
83. When first visiting the Website or App, the user is prompted to create an account. The user must select which type of account they would like to create (i.e. a "personal" investing account.)

84. Using the technology described above, this information is transmitted to each Third Party as it is selected on the Website or App.

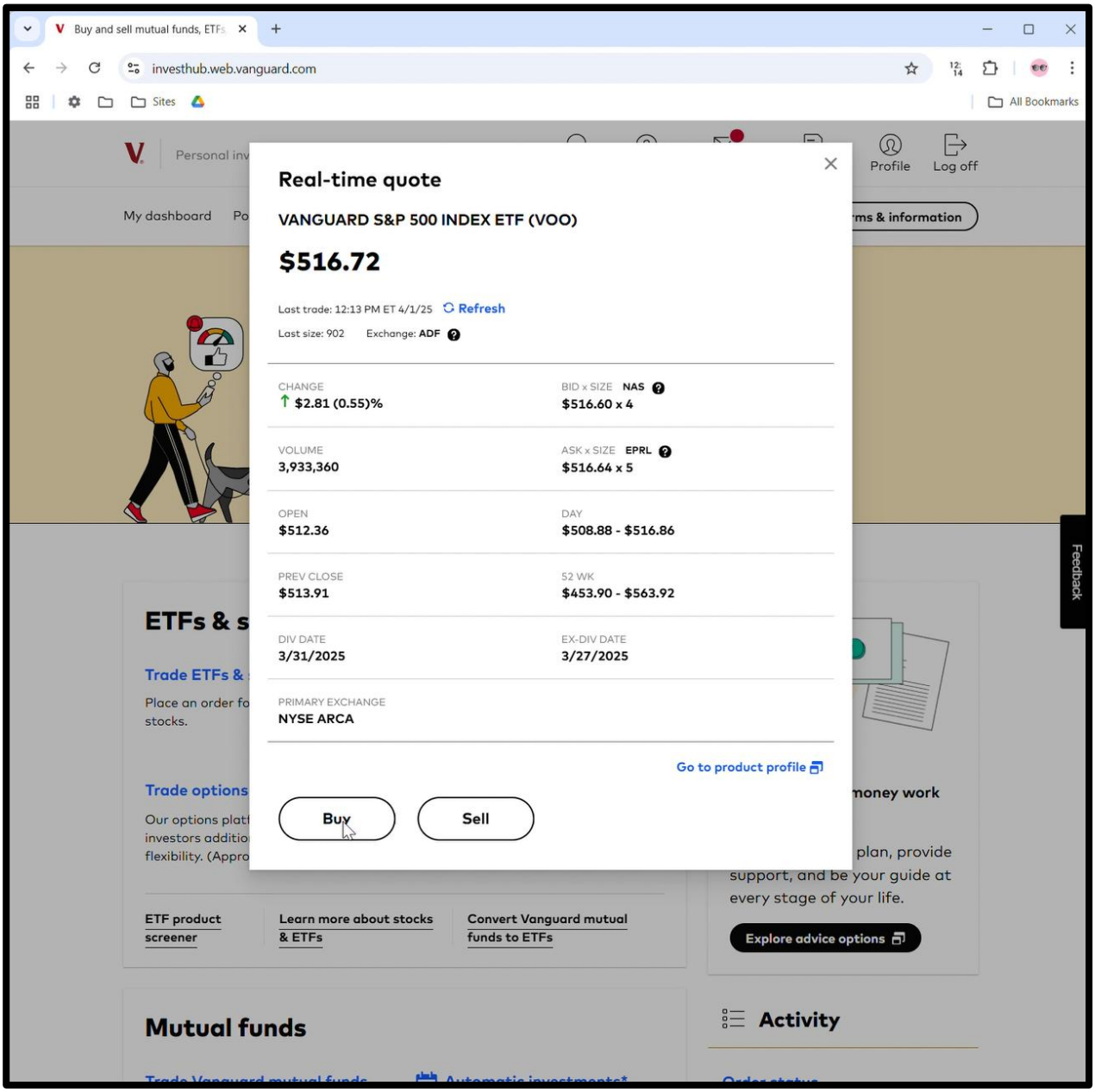
85. The image below shows the transmission of the account selection to Meta, via the Facebook Pixel, when selected on the Website. The "open-account" address indicates the user is creating an account and the "perosnal1" address shows the selection for a personal investment account.

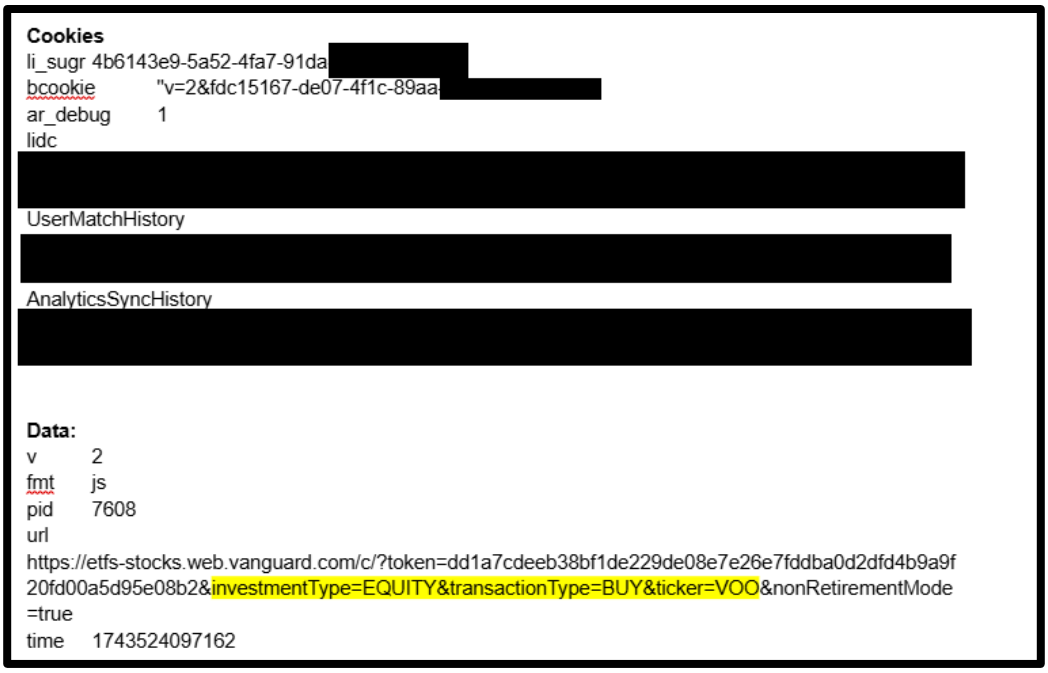


86. The image below shows the same transmission from the App. The address is the same "web.vanguard" address because the App opens a web browser for the account creation process.



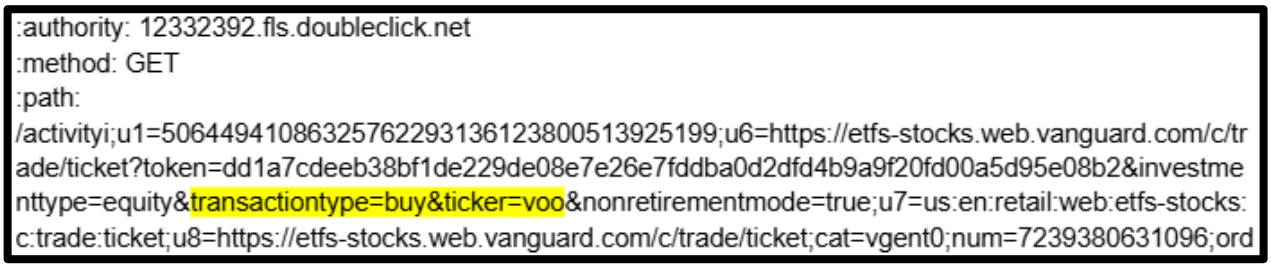
87. When a user logs in to their account and selects investments, every selection the user makes is tracked through the page URL, which identifies a purchase is being made and which fund or stock is being purchased. Through the trackers installed on the Website, the Third Parties intercept all responses entered by users, in real time, as shown below. For example, LinkedIn and Google intercept each stage of a user's selection of Domestic Stock for investment, the ticker name, and the action the user is taking with this investment.





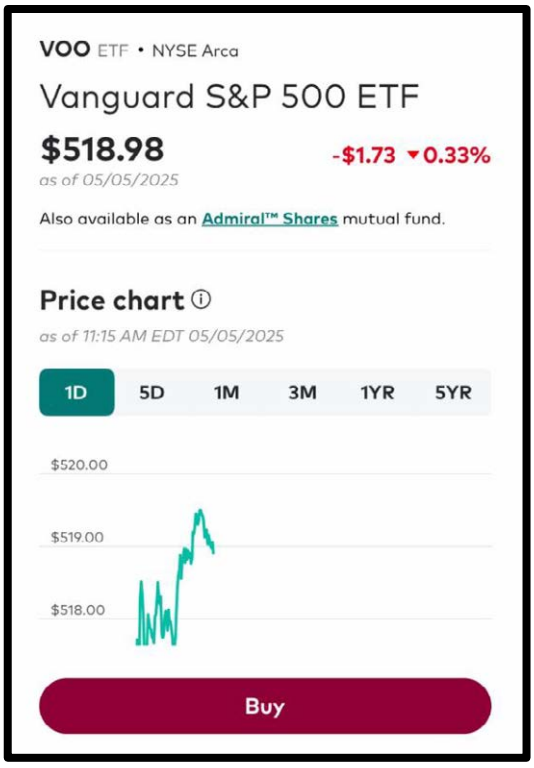
Cookies
li_sugr 4b6143e9-5a52-4fa7-91da[redacted]
bcookie "v=2&fdc15167-de07-4f1c-89aa[redacted]
ar_debug 1
lidc
[redacted]
UserMatchHistory
[redacted]
AnalyticsSyncHistory
[redacted]

Data:
v 2
fmt js
pid 7608
url
https://etfs-stocks.web.vanguard.com/c/?token=dd1a7cdeeb38bf1de229de08e7e26e7fddba0d2dfd4b9a9f20fd00a5d95e08b2&investmentType=EQUITY&transactionType=BUY&ticker=VOO&nonRetirementMode=true
time 1743524097162



:authority: 12332392.fls.doubleclick.net
:method: GET
:path:
/activityi;u1=5064494108632576229313612380051392519 9;u6=https://etfs-stocks.web.vanguard.com/c/trade/ticket?token=dd1a7cdeeb38bf1de229de08e7e26e7fddba0d2dfd4b9a9f20fd00a5d95e08b2&investmenttype=equity&transactiontype=buy&ticker=voo&nonretirementmode=true;u7=us:en:retail:web:etfs-stocks:c:trade:ticket;u8=https://etfs-stocks.web.vanguard.com/c/trade/ticket;cat=vgent0;num=7239380631096;ord

88. The same is true regarding purchases on the App. A record of each purchase, including the ticker of the fund purchased, is sent in real time to LinkedIn and Google.



Adservice Google- VOO BUY
adservice.google.com
Mon May 05 11:31:29 EDT 2025

GET
/ddm/fls/z/u1=0718933862158987279138821068908278981O;u6=https://etfs-stocks.web.vanguard.com/c/trade/ticket?token=dd1a7cdeeb38bf1de229de08e7e26e7fddba0d2dfd4b9a9f20fd00a5d95e08b2&transactiontype=buy&ticker=voo;u7=us:en:retail:web:etfs-stocks:c;u8=https://etfs-stocks.web.vanguard.com/c/trade/ticket;cat=vgent0;num=3672705579187;ord=1;src=12332392;gdpr=${GDPR};type=allla0;gdpr_consent=

LinkedIn- VOO BUY
px.ads.linkedin.com
Mon May 05 11:31:28 EDT 2025

REQUEST DATA:
v 2
fmt js
pid 7608
url
https://etfs-stocks.web.vanguard.com/c/trade/ticket?token=dd1a7cdeeb38bf1de229de08e7e26e7fddba0d2dfd4b9a9f20fd00a5d95e08b2&transactionType=BUY&ticker=VOO
time 1746459088312

89. Additionally, every search query a user enters into Defendant's Website and App collected and transmitted to LinkedIn and Google.

px.ads.linkedin.com
/collect?v=2&fmt=js&pid=7608&url=https://investor.vanguard.com/search#q=etf vs mutual fund&time=1743524258447
Tue Apr 01 12:17:38 EDT 2025

12332392.fls.doubleclick.net
/activityi;dc_pre=CLDcw4Cet4wDFTytWgUdcQE9nw;u1=5064494108632576229313612380051392519 9;u6=https%3A%2F%2Finvestor.vanguard.com%2Fsearch%23q%3Detf%2520vs%2520mutual%2520fund;u7=us%3Aen%3Aretail%3Aweb%3Ainvestor%3Asearch;u8=https%3A%2F%2Finvestor.vanguard.com%2Fsearch;cat=vgent0;num=2774698057641;ord=1;src=12332392;gdpr=%24%7BGDPR%7D;type=allla0;gdpr_consent=%24%7BGDPR_CONSENT_755%7D
Tue Apr 01 12:17:38 EDT 2025

90. Each purchase, search, or communication with Defendant's Website or App is linked to an individual using the cookies and other identifying information described above.

91. Each interception happened in real time as the information was entered into or selection was made on the Website or App.

92. Each Third Party viewed each and every piece of information, processed it, assembled it into datasets, and used it in their respective advertising services as described above.

III. DEFENDANT INTERCEPTED AND DISCLOSED PLAINTIFFS' PROTECTED ELECTRONIC COMMUNICATIONS FOR MARKETING, ADVERTISING, AND ANALYTICS PURPOSES

A. Defendant Disclosed Users' Information to LinkedIn for Marketing, Advertising, and Analytics Purposes

93. As described above, Defendant intercepts consumers' confidential communications through the LinkedIn Insight Tag.

94. The purpose of this invasion of privacy is straightforward: Defendant discloses this protected information to LinkedIn for marketing purposes.

95. This is valuable to Defendant because it improves the effectiveness of Defendant's advertisements, allows for the targeting of users, and provides performance information for ad campaigns.

96. In addition to helping companies like Defendant make better use of their own customers' information, LinkedIn aggregates that information with the information collected from all sites containing the LinkedIn Insight Tag to track users across multiple websites and platforms, which increases the value of LinkedIn's advertising services when they are offered to other companies.

97. Thus, Defendant's disclosure of consumer information is done for the purpose of improperly increasing its own advertising efficiency, as well as LinkedIn's.

B. Defendant Disclosed Users' Information to Google Analytics for Marketing, Advertising, and Analytics Purposes

98. As described above, through the Google Analytics tracking code, Defendant intercepts consumers' confidential communications.

99. The purpose of this invasion of privacy is straightforward: Defendant discloses this protected information to Google for marketing purposes.

100. This is valuable to Defendant because it improves the effectiveness of Defendant's advertisements, allows for the targeting of users, and provides performance information for ad campaigns.

101. In addition to helping companies like Defendant make better use of their own customers' information, Google aggregates that information with the information collected from all sites containing the Google Analytics tracking code to track users across multiple websites and platforms, which increases the value of Google's advertising services when they are offered to other companies.

102. Thus, Defendant's disclosure of consumer information is done for the purpose of improperly increasing its own advertising efficiency, as well as Google's.

C. Defendant Disclosed Users' Information to Meta for Marketing, Advertising, and Analytics Purposes

103. As described above, through the Meta Pixel, Defendant intercepts consumers' confidential communications .

104. The purpose of this invasion of privacy is straightforward: Defendant discloses this protected information to Meta for marketing purposes.

105. This is valuable to Defendant because it improves the effectiveness of Defendant's advertisements, allows for the targeting of users, and provides performance information for ad campaigns.

106. In addition to helping companies like Defendant make better use of their own customers' information, Meta aggregates that information with the information collected from all sites containing the Meta Pixel to track users across multiple websites and platforms, which increases the value of Meta's advertising services when they are offered to other companies.

107. Thus, Defendant's disclosure of consumer information is done for the purpose of improperly increasing its own advertising efficiency, as well as Meta's.

IV. PLAINTIFFS AND CLASS MEMBERS WERE INJURED BY DEFENDANT'S BREACH OF THEIR PRIVACY

108. "Individuals have a time-honored right to control access to their private information and affairs." *Frasco v. Flo Health, Inc.*, 2025 WL 1433825, at *11 (N.D. Cal. May 19, 2025). "Likewise, 'Congress has long provided plaintiffs with the right to seek redress for unauthorized disclosures of information that, in Congress's judgment, ought to remain private.'" *In re Google Inc. Cookie Placement Consumer Privacy Litig*. 934 F.3d 316, 325 (3d Cir. 2019).

109. As evidenced by the GLBA and other laws, financial information and information that is supposed to be safeguarded by financial institutions, is information explicitly defined as the type of information that "ought to remain private" and for which individuals can and should seek redress if improper disclosure occurs.

110. Defendant disclosed Plaintiffs' and Class Members' highly sensitive financial information, including their trades and purchases of financial products. The loss of this information is part-and-parcel of Plaintiffs' and Class Members' loss of the right to control their private affairs, including financial transactions.

111. Accordingly, Plaintiffs and Class Members have suffered concrete injuries as a result of Defendant's conduct.

CLASS ALLEGATIONS

112. Plaintiffs bring this action on behalf of all consumers in the United States who hold a personal investment or workplace retirement account with Vanguard who have accessed the Website in the following Classes (collectively, the "Classes"):

Nationwide Class. All natural persons in the United States who, during the determined Class Period, had their protected personal and financial information disclosed through the Website or App to Third Parties.

California Subclass. All natural persons in California who, during the determined Class Period, had their protected personal and financial information disclosed through the Website or App to Third Parties.

Pennsylvania Subclass. All natural persons in the Commonwealth of Pennsylvania who, during the determined Class Period, had their protected personal and financial information disclosed through the Website or App to Third Parties.

113. Excluded from the Class is Defendant, the officers and directors of the Defendant at all relevant times, members of their immediate families and their legal representatives, heirs, successors, or assigns and any entity in which either Defendant has or had a controlling interest.

114. Plaintiffs are members of the Class they seek to represent.

115. Members of the putative Class are so numerous that their individual joinder herein is impracticable. Based on information and Plaintiffs' belief, members of the putative Class number in the millions. The precise number of putative Class members and their identities are unknown to Plaintiffs at this time but may be determined through discovery. Putative Class members may be notified of the pendency of this action by mail and/or publication through the distribution of Defendant's records.

116. Common questions of law and fact exist as to all putative Class members and predominate over questions affecting only individual Class members. Common legal and factual questions include, but are not limited to:

(a) Whether Vanguard's conduct violates the Electronic Communications Privacy Act, 18 U.S.C. § 2511(1), *et seq.*;

(b) Whether Vanguard's conduct violates the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. § 5701, *et seq.*;

(c) Whether Vanguard's conduct violates the California Invasion of Privacy Act, Cal. Penal Code § 630, *et seq*.;

(d) Whether Third Parties learned the contents of Plaintiffs' and Class members' communications with Vanguard;

(e) Whether Third Parties used the information it learned from the contents of Plaintiff's and Class members' communications with Vanguard; and

(f) Whether Third Parties intentionally used an electronic amplifying or recording device to eavesdrop or record Plaintiffs' and Class members' confidential communications with Vanguard without the Plaintiffs' and Class members' consent.

117. Plaintiffs' claims are typical of the claims of the members of the Class as all members of the Class are similarly affected by Defendant's wrongful conduct. Plaintiffs have no interests antagonistic to the interests of the other members of the Class. Plaintiffs and all members of the Class have sustained economic injury arising out of Defendant's violations of statutory law as alleged herein.

118. Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the putative Class members they seek to represent, they have retained counsel competent and experienced in prosecuting class actions, and they intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

119. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Plaintiffs and the putative members of the Class. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Even if every member of the Classes could afford to pursue individual litigation, the court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents potential for inconsistent or

contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims are consistently adjudicated.

120. Plaintiffs reserve the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

COUNT I
Violation of the Electronic Communications Privacy Act
18 U.S.C. § 2511(1), *et seq.*
(On Behalf of the Nationwide Class)

121. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein and bring this count individually and on behalf of the members of the Nationwide Class against Defendant.

122. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

123. The ECPA protects both sending and receiving communications.

124. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

125. The transmission of Plaintiffs' personally identifying information ("PII") to Defendant's Website qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(12).

126. The transmission of PII from Plaintiffs and Class members to Defendant's Website, with which they chose to exchange communications are "transfer[s] of signs, signals,

writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

127. The ECPA defines "contents," when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. 18 U.S.C. § 2510(8).

128. The ECPA defines an interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

129. The ECPA defines "electronic, mechanical, or other device," as "any device…which can be used to intercept a[n]…electronic communication[.]" 18 U.S.C. § 2510(5).

130. The following instruments constitute "devices" within the meaning of the ECPA:

a. The computer codes and programs Defendant and Third Parties used to track Plaintiffs' and Class members' communications while they were navigating the Website and App;

b. Plaintiffs' and Class members' browsers;

c. Plaintiffs' and Class members' mobile devices;

d. Defendant and Third Parties' web and ad servers;

e. The plan Defendant and Third Parties carried out to effectuate the tracking and interception of Plaintiffs' and Class members' communications while they were using a web browser to navigate the Website.

131. Plaintiffs' and Class members' interactions with Defendant's Website are electronic communications under the ECPA.

132. By utilizing and embedding the tracking technology provided by Third Parties on its Website, Defendant intentionally intercepted, endeavored to intercept, and/or procured another person to intercept the electronic communications of Plaintiffs and Class members in violation of 18 U.S.C. § 2511(1)(a).

133. Specifically, Defendant intercepted—in real time—Plaintiffs' and Class members' electronic communications via the tracking technology provided by Google on its Website, which tracked, stored and unlawfully disclosed Plaintiff's and Class Members' PII to Third Parties.

134. Defendant intercepted communications that include, but are not necessarily limited to, communications to/from Plaintiffs and Class members regarding PII, including their identities and information related to their financial holdings. This confidential information is then monetized for targeted advertising purposes, among other things.

135. By intentionally disclosing or endeavoring to disclose Plaintiffs' and Class members' electronic communications to affiliates and other Third Parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

136. By intentionally using, or endeavoring to use, the contents of Plaintiffs' and Class members' electronic communications, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

137. Defendant intentionally intercepted the contents of Plaintiffs' and Class members' electronic communications for the purpose of committing a criminal or tortious act in violation of the Constitution or laws of the United States or of any state, namely, invasion of privacy, among others.

138. The party exception in 18 U.S.C. § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State. Here, as alleged above, "[t]he association of Plaintiffs' data with preexisting user profiles is a further use of Plaintiffs' data that satisfies [the crime-tort] exception," because it "violate[s] state law, including the [CIPA and WESCA], intrusion upon seclusion, and invasion of privacy." *Brown v. Google, LLC*, 525 F. Supp. 3d 1049, 1067 (N.D. Cal. 2021); *see also Riganian v. Liveramp Holdings, Inc.*, ---F.Supp.3d---, 2025 WL 2021802, at *9-10 (N.D. Cal. July 18, 2025); *Marden v.LMND Medical Group, Inc.*, 2024 WL 4448684, at *2 (N.D. Cal. July 3, 2024); *R.C. v. Walgreen Co.*, 733 F. Supp. 3d 876, 902 (C.D. Cal. 2024).

139. In addition, Defendant violated a provision of the Gramm-Leach-Bliley Act, 16 C.F.R. § 313. This provision imposes a criminal penalty for knowingly disclosing "nonpublic personal information" to a third party. GLBA defines nonpublic personal information as:

> Any information that is not publicly available and that: a consumer provides a financial institution to obtain a financial product or service from the institution; results from a transaction between the consumer and the institution involving a financial product or service; or a financial institution otherwise obtains about a consumer in connection with providing a financial product or service.[58]

[58] 16 C.F.R. § 313

140. Defendant was not acting under the color of law to intercept Plaintiffs' and Class members' wire or electronic communications.

141. Plaintiffs and Class members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiffs' and Class members' privacy. Plaintiffs and Class members had a reasonable expectation that Defendant would not redirect their communications to Third Parties without their knowledge or consent.

142. The foregoing acts and omission therefore constitute numerous violations of 18 U.S.C. § 2511(1), *et seq*.

143. As a result of each and every violation thereof, on behalf of themselves and the Class, Plaintiffs seek statutory damages of $10,000, or $100 per day for each violation of 18 U.S.C. § 2510, *et seq*., under 18 U.S.C. § 2520.

COUNT II
Violation of the Pennsylvania Wiretapping and Electronic Surveillance Control Act
18 Pa. Cons. Stat. § 5701, *et seq.*
(On Behalf Of The Pennsylvania Subclass)

144. Plaintiff Dy incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein. Plaintiff Dy repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the Pennsylvania Subclass against Defendant.

145. The Pennsylvania Wiretapping and Electronic Surveillance Control Act ("WESCA") prohibits (1) the interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication; and (3) the intentional use of the contents of any wire, electronic, or oral communication that the discloser knew or should

have known was obtained through the interception of a wire, electronic, or oral communication. 18 Pa. Cons. Stat. § 5703.

146. Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use, a wire, electronic, or oral communication in violation of the Act is subject to a civil action for (1) actual damages, not less than liquidated damages computed at a rate of $100 per day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred. 18 Pa. Cons. Stat. § 5725(a).

147. Defendant's Terms and Conditions of Use, made available to all investors in the United States, state that "The laws of the Commonwealth of Pennsylvania, United States of America, without regard to principles of conflict of laws, govern these Terms of Use and any dispute that might arise between you and Vanguard. If you take legal action relating to these Terms of Use, you agree to file such action either in the Court of Common Pleas of Chester County, Pennsylvania, or the United States District Court for the Eastern District of Pennsylvania[.]"[59] As such, the WESCA applies to Defendant's conduct as to the entire Nationwide Class.

148. At all relevant times, Defendant procured the Third Parties to track and intercept Plaintiffs' and Class members' internet communications while navigating the Website that Defendant owns and operates.

149. Defendant, when procuring the Third Parties to intercept Plaintiffs' communications, intended for the Third Parties to learn the meaning of the content that Website visitors requested.

150. At all relevant times, the Third Parties intentionally used the intercepted

[59] https://investor.vanguard.com/terms-conditions.

communications for their own purposes, including to improve the Third Parties' own products and services.

151. The wiretapping of Plaintiff Dy's and Class Members occurred in Pennsylvania, where the Third Parties—as enabled by Defendant—routed Plaintiff Dy's and Pennsylvania Subclass Members' electronic communications from Defendant's servers.

152. These communications were intercepted without authorization and consent from Plaintiff Dy and Class Members. Plaintiff Dy and Class Members did not provide their prior consent to the Third Parties' intentional access, interception, reading, learning, recording, collection, and usage of Plaintiff Dy's and Pennsylvania Subclass Members' electronic communications. Nor did Plaintiff Dy and Pennsylvania Subclass Members provide their prior consent to Defendant's procuring the Third Parties for the foregoing.

153. Plaintiff Dy and Pennsylvania Subclass Members were not aware that their electronic communications were being intercepted by the Third Parties.

154. Plaintiffs and Class Members had a justified expectation under the circumstances that their electronic communications would not be intercepted. Said electronic communications consisted of "nonpublic personal information," as defined by 16 C.F.R. § 313.3 (the Gramm-Leach-Biley Act).

155. Plaintiff Dy and Pennsylvania Subclass Members have been injured by Defendant's WESCA violations, and pursuant to 18 Pa. Cons. Stat. § 5725(a), each seeks statutory damages of $1,000 for each of Defendant's violations of WESCA.

COUNT III
Violation of the California Invasion of Privacy Act,
Cal. Penal Code § 631
(On Behalf of the California Subclass)

156. Plaintiffs Felsen and Ragusano repeat the allegations contained in the paragraphs above as if fully set forth herein and bring this count individually and on behalf of the members of the California Subclass against Defendant.

157. The California Invasion of Privacy Act (the "CIPA") is codified at California Penal Code Sections 630 to 638. The CIPA begins with its statement of purpose—namely, that the purpose of the CIPA is to "protect the right of privacy of the people of [California]" from the threat posed by "advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications . . ." Cal. Penal Code § 630.

158. A person violates California Penal Code Section 631(a) if:

> by means of any machine, instrument, or contrivance, or in any other manner, [s/he] intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or [s/he] willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or [s/he] uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained . . .[60]

159. To avoid liability under section 631(a), a defendant must show it had the consent of <u>all</u> parties to a communication.

[60] Cal. Penal Code § 631(a).

160. At all relevant times, Third Parties tracked and intercepted Plaintiffs' and California Subclass members' internet communications while using the Website and the App as Plaintiffs and Class members made investment and financial planning decisions. These communications were intercepted without the authorization and consent of Plaintiffs and California Subclass members.

161. Through these interceptions, Third Parties intended to learn some meaning of the content the consumers communicated.

162. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, the LinkedIn Insight Tag and the Google Analytics Pixel fall under the broad catch-all category of "any other manner":

a. The computer codes and programs LinkedIn and Google used to track Plaintiffs and California Subclass members' communications while they were navigating the Website and the App;

b. The computer codes and programs the Third Parties used to track Plaintiffs' and California Subclass members' communications while they were navigating the Website and the App;

c. Plaintiffs' and California Subclass members' browsers;

d. Plaintiffs' and California Subclass members' computing and mobile devices;

e. Third Parties' web and ad servers;

f. The web and ad servers from which Third Parties tracked and intercepted Plaintiffs' and California Subclass members' communications while they were using a web browser to access or navigate the Website;

g. The computer codes and programs used by Third Parties to effectuate their tracking and interception of Plaintiffs' and California Subclass members' communications while they were using a browser to visit the Website or use the App; and

h. The plan Third Parties carried out to effectuate its tracking and interception of Plaintiffs' and California Subclass members' communications while they were using a web browser or mobile device to visit the Website or use the App.

163. At all relevant times, Third Parties, through their associated tracking technologies, intentionally tapped or made unauthorized connections with the lines of internet communications between Plaintiffs and California Subclass members and the Vanguard Website and App without the consent of all parties to the communication.

164. Third Parties, willfully and without the consent of Plaintiffs and California Subclass members, read or attempted to read, or learn the contents or meaning of Plaintiffs' and California Subclass members' communications to Vanguard while the communications are in transit or passing over any wire, line or able, or were being received at any place within California when it intercepted Plaintiffs' and California Subclass members' communications and data with Vanguard.

165. Third Parties used or attempted to use the communications and information they received through their tracking technology, including to supply advertising services.

166. The confidential information intercepted through the Third Parties' tracking technologies, including but not limited to investment and financial planning decisions, constituted protected personal information.

167. As a result of the above violations, Defendant is liable to Plaintiffs Felsen and

Ragusano and other California Subclass members in the amount of $5,000 dollars per violation or three times the amount of actual damages, whichever is greater. Additionally, California Penal Code Section 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages."

168. Under the CIPA, Defendant is also liable for reasonable attorney's fees and other litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendant in the future.

COUNT IV
Violation of the California Invasion of Privacy Act,
Cal. Penal Code § 632
(On Behalf of the California Subclass)

169. Plaintiffs Felsen and Ragusano repeat the allegations contained in the paragraphs above as if fully set forth herein and bring this count individually and on behalf of the members of the California Subclass against Defendant.

170. Cal. Penal Code section 632 prohibits "intentionally and without the consent of all parties to a confidential communication," the "use[] [of] an electronic amplifying or recording device to eavesdrop upon or record the confidential communication."

171. Section 632 defines "confidential communication" as "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto[.]"

172. Plaintiffs' and California Subclass members' communications to Vanguard, including their sensitive personal and financial information, were confidential communications for purposes of section 632, because Plaintiffs and Class members had an objectively reasonable expectation of privacy in this data.

173. Plaintiffs and California Subclass members expected their communications to Vanguard to be confined to Vanguard in part due to the protected nature of the information at issue. Plaintiffs and Class members did not expect Third Parties to secretly eavesdrop upon or record this confidential information and their communications.

174. Third Party tracking technology, i.e., the LinkedIn Insight Tag, Google Analytics Pixel, and Meta Pixel, are electronic amplifying or recording devices for purposes of section 632.

175. By contemporaneously intercepting and recording Plaintiffs' and California Subclass members' confidential communications to Vanguard through this technology, Third Parties eavesdropped and/or recorded confidential communications through an electronic amplifying or recording device in violation of section 632 of CIPA.

176. At no time did Plaintiffs Felsen and Ragusano or California Subclass members consent to Third Parties' conduct, nor could they reasonably expect that their communications to Vanguard would be overheard or recorded by Third Parties.

177. The Third Parties utilized Plaintiffs' and California Subclass members' sensitive personal and financial information for their own purposes, including for targeted advertising.

178. Plaintiffs Felsen and Ragusano and California Subclass members seek statutory damages in accordance with section 637.2(a) which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiffs and the Class in an amount to be proven at trial, as well as injunctive or other equitable relief.

179. Plaintiffs Felsen and Ragusano and California Subclass members have also suffered irreparable injury from these unauthorized acts. Plaintiffs' and Class members' sensitive data has been collected, viewed, accessed, and stored by Third Parties. This sensitive data has not been destroyed, and due to the continuing threat of such injury, Plaintiffs and Class

members have no adequate remedy at law. Plaintiffs and Class members are accordingly entitled to injunctive relief.

COUNT V
Invasion of Privacy Under California's Constitution/ Intrusion Upon Seclusion
(On Behalf of the California Subclass)

180. Plaintiffs Felsen and Ragusano repeat the allegations contained in the paragraphs above as if fully set forth herein and bring this count individually and on behalf of the members of the California Subclass against Defendant.

181. Plaintiffs Felsen and Ragusano and California Subclass members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications and protected financial information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion, or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to wiretaps without Plaintiffs' and Class members' knowledge or consent.

182. At all relevant times, by using the Third Party tracking technologies to record and communicate users' personal identifiers alongside their sensitive personal information and confidential medical communications, Defendant intentionally invaded Plaintiffs' and Class members' privacy rights under the California Constitution and intruded upon their seclusion.

183. Plaintiffs Felsen and Ragusano and Class members had a reasonable expectation that their communications, identities, financial information, and other data would remain confidential, and that Defendant would not intercept such information communicated on its Website.

184. Plaintiffs Felsen and Ragusano and Class members did not authorize Defendant to record and transmit Plaintiffs' and Class members' private financial communications alongside their personally identifiable information.

185. This invasion of privacy was serious in nature, scope, and impact because it related to users' private financial communications. Moreover, it constituted an egregious breach of the societal norms underlying the privacy right.

186. Accordingly, Plaintiffs Felsen and Ragusano and California Subclass members seek all relief available for invasion of privacy under the California Constitution and common law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for relief and judgment, as follows:

A. For a determination that this action is a proper class action;

B. For an order certifying the Classes, naming Plaintiffs as representatives of the Class, and naming Plaintiffs' attorneys as Class Counsel to represent the Class;

C. For an order declaring that Defendant's conduct violated the statutes referenced herein;

D. For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

E. For an award of compensatory damages, including statutory damages where available, to Plaintiffs and the Class members against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial;

F. For punitive damages, as warranted, in an amount to be determined at trial;

G. For an order requiring Defendant to disgorge revenues and profits

wrongfully obtained;

H. For prejudgment interest on all amounts awarded;

I. For injunctive relief as pleaded or as the Court may deem proper;

J. For an order awarding Plaintiffs and the Class their reasonable attorneys' fees and expenses and costs of suit; and

K. For an order granting Plaintiffs and Class members such further relief as the Court deems appropriate.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: July 25, 2025

Respectfully submitted,

By: */s/ Mark C. Atlee*

ATLEE HALL, LLP
Mark C. Atlee (PA No. 204627)
415 North Duke Street
Lancaster, PA 17602
Telephone: (717) 393-9596
Facsimile: (717) 393-2138
E-mail: mcatlee@atleehall.com

BURSOR & FISHER, P.A.
Alec M. Leslie *(pro hac vice* application forthcoming)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163
E-Mail: aleslie@bursor.com

Attorneys for Plaintiffs and the Putative Class