Natalie Lyons, No. 293026
Vess A. Miller, No. 278020
Lynn A. Toops*
Amina A. Thomas*
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
Tel: (317) 636-6481
nlyons@cohenandmalad.com
ltoops@cohenandmalad.com
*To move for *pro hac vice* admission
[*additional counsel listed on signature pages*]
***Counsel for Plaintiff and Proposed Class***

**UNITED STATES DISTRICT COURT**
**NORTHERN DISTRICT OF CALIFORNIA**
**SAN FRANCISCO DIVISION**

| | |
|---|---|
| **VISHAL SHAH, GARY INGRAHAM, DEIA WILLIAMS, and DEVIN ROSE, individually, and on behalf of all others similarly situated,**<br><br>**Plaintiffs**<br><br>**v.**<br><br>**CAPITAL ONE FINANCIAL CORPORATION, d/b/a CAPITAL ONE, d/b/a CAPITAL ONE, NATIONAL ASSOCIATION, d/b/a CAPITAL ONE, N.A., d/b/a CAPITAL ONE SHOPPING**<br><br>**Defendant.** | **Civil Action No. _____**<br><br>**CLASS ACTION COMPLAINT FOR:**<br>**1. Negligence**<br>**2. Negligence Per Se**<br>**3. Invasion of Privacy**<br>**4. Violation of Comprehensive Computer Data Access and Fraud Act, Cal. Pen. Code § 502**<br>**5. Violation of Consumer Protection Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.***<br>**6. Violation of Consumer Privacy Act, Cal. Civ. Code, §§ 1798.100, *et seq.***<br>***7.* Violation of Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.***<br>**8. Breach of Express and Implied Contract**<br>**9. Unjust Enrichment**<br>**10. Bailment**<br>**11. Declaratory Judgment**<br>**12. Breach of Confidence**<br>**13. Violation of Invasion of Privacy Act, Cal. Pen. Code §§ 630, *et seq*.**<br>**14. Violations of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2511(1), *et seq.* and 18 U.S.C. § 2702, *et seq.***<br>**15. Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq.***<br><br>**DEMAND FOR JURY TRIAL** |

## CLASS ACTION COMPLAINT

Plaintiffs, Vishal Shah, Gary Ingraham, Deia Williams, and Devin Rose, individually, and on behalf of all others similarly situated (hereinafter "Plaintiffs") bring this Class Action Complaint against Defendant, Capital One Financial Corporation, d/b/a Capital One, National Association ("Capital One" or "Defendant"), and allege, upon personal knowledge as to their own actions, and upon information and belief as to all other matters, as follows.

## INTRODUCTION

1. Plaintiffs bring this class action to address Defendant's outrageous, illegal, and widespread practice of disclosing—without consent—the Nonpublic Personal Information[1] and Personally Identifiable Financial Information[2] (together, "Personal and Financial Information") of Plaintiffs and the proposed Class Members to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook" or "Meta"), Google, LLC ("Google"), Microsoft Corp. ("Microsoft"), DoubleClick, NewRelic, Adobe, Everest, Skai/Kenshoo, Snowplow, BioCatch, Tealium, and possibly others (collectively the "Third Parties") (in short, "the Disclosure").

2. Capital One is a massive financial institution which provides financial services to customers across the globe and the United States, including in California and Virginia. To provide these services, Capital One operates and encourages its customers to use its website,

[1] The United States Congress defines "nonpublic personal information" as "personally identifiable financial information-- (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution." The Gramm-Leach-Bliley Act, 15 U.S.C.A. § 6809(4)(A) ("GLBA").

[2] "Personally identifiable financial information means any information: (i) A consumer provides to [a financial institution] to obtain a financial product or service from [the financial institution]; (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." 16 C.F.R. § 313.3(o)(1).

https://www.CapitalOne.com (the "Website"), on which customers can access their account information, access Capital One's financial services, and apply for financial products like credit cards.

3. Despite its unique position as a massive and trusted bank, Capital One used its Website to blatantly collect and disclose Consumers'[3] and Customers'[4] (collectively, "Customers") Personal and Financial Information to Third Parties uninvolved in the provision of financial services—entirely without their knowledge or authorization. Capital One did so by knowingly and secretly configuring and implementing code-based tracking devices ("trackers" or "tracking technologies") into its Website.

4. Through these trackers, Capital One disclosed and continues to disclose Personal and Financial Information that Customers input into and accessed on Capital One's Website. This information includes without limitation account information, credit card application information, and credit card pre-approval information, including the fact that a user was on a certain page, that users clicked buttons and what URLs or webpages they led to, information entered on preapproval application pages including their employment information, bank account information, and Customers' eligibility, preapproval, or approval for a credit card.

5. Upon information and belief, Capital One utilized data from trackers to improve and to save costs on its marketing campaigns, improve its data analytics, attract new customers,

[3] The term "consumer" means "an individual who obtains or has obtained a financial product or service from [a financial institution] that is to be used primarily for personal, family, or household purposes, or that individual's legal representative." 16 C.F.R. § 313.3; 15 U.S.C.A. § 6809(9).

[4] "Customer means a consumer who has a customer relationship with [a financial institution]." 16 C.F.R. § 313.3. "The term "time of establishing a customer relationship" shall . . . in the case of a financial institution engaged in extending credit directly to consumers to finance purchases of goods or services, mean the time of establishing the credit relationship with the consumer." 15 U.S.C.A. § 6809.

and generate sales. Capital One benefited from use of Customers' Personal and Financial Information. Capital One further allowed the Third Parties, who are uninvolved in Capital One's provision of financial services, to profit from its Disclosure of Customers' Private and Financial information. And the Third Parties used Customers' Personal and Financial Information for themselves and disclosed to fourth parties who also profited off of it. Facebook, for example, will use the data collected from Customers of Capital One to sell ads to fourth parties who will profit off of the use of that information

6. Customers, like Plaintiffs and Class Members, simply do not anticipate that a trusted financial institution will send their Personal and Financial Information to hidden Third Parties (who in turn share with fourth parties), all of whom profit off of it; likewise, when Plaintiffs and Class Members used Defendant's Website, they thought they were communicating exclusively with a trusted financial institution.

7. At no time did Capital One disclose to Plaintiffs or Class Members that they were sharing their Personal and Financial Information with the Third Parties for third- and fourth-party use. Plaintiffs and Class Members never signed a written authorization permitting Defendant to send their Personal and Financial Information to the Third Parties who were uninvolved in the provision of financial services. And Capital One never allowed Plaintiffs or Class Members a real opportunity to opt-out of its Disclosure.

8. Defendant owed a variety of duties, including common law, statutory, contractual, and regulatory duties, to keep Plaintiffs' and Class Members' Personal and Financial Information safe, secure, and confidential.

9. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Personal and Financial Information, Defendant assumed legal and equitable duties to those individuals to protect and safeguard their information from unauthorized disclosure.

10. The statutory and regulatory duties Capital One owed Customers include its obligations under federal law. For example, the GLBA requires that "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C.A. § 6801. Under this federal law, financial institutions like Capital One are explicitly prohibited from disclosing a Customer's Personal and Financial Information without sufficient advance notification and opt-out opportunity. 15 U.S.C.A. § 6801, *et seq*.

11. Capital One ignored all its duties and obligations, including the GLBA's prohibition, by disclosing Customers' Personal and Financial Information without proper advance notification and opt-out rights as required under the GLBA.

12. Examples of "Personal and Financial Information" included in the GLBA are indistinguishable from the types of information Capital One disclosed to Facebook, including, among other things: (a) "[i]nformation a consumer provides to [Capital One] on an application to obtain a loan, credit card, or other financial product or service"; (b) "[t]he fact that an individual is or has been one of [Capital One's] customers or has obtained a financial product or service from [Capital One]"; (c) "information about [Capital One's] consumer . . . disclosed in a manner that indicates that the individual is or has been [Capital One's] consumer"; (d) "information that a consumer provides to [Capital One] or that [Capital One] or [its] agent otherwise obtain[s] in connection with collecting on, or servicing, a credit account"; "[a]ny information that a consumer provides to [Capital One] or that [Capital One] or [its] agent otherwise obtain[s] in connection

with collecting on, or servicing, a credit account; and (e) "any information [Capital One] collect[s] through an Internet 'cookie' (an information collecting device from a web server)." 16 C.F.R. 313.3(o)(2)(i).

13. Capital One breached its duties under California state law, including, for example, the California Consumer Privacy Act. That statue provides California consumers with rights to control their personal information including the right to know what personal information is being collected about them and whether that information is sold or disclosed and to whom, the right to prohibit the sale of their personal information, and the right to request deletion of their personal information. Cal. Civ. Code § 1798.100 *et seq*. Capital One breached its obligations under this statute by, for example, failing to provide Customers with appropriate notice that their information was being disclosed to Third Parties for third- and fourth- party use. The notice and consent Capital One purports to provide and obtain, through the policies it provides on its website, is not appropriate, as a reasonable Consumer would not have understood those policies as notifying them of Capital One's disclosure of their Personal and Financial Information to Third Parties for third- and fourth- party use.

14. Capital One breached its common law, statutory, and contractual obligations to Plaintiffs and Class Members by, *inter alia*, (i) failing to adequately review its marketing programs and web based technology to ensure its Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share Personal and Financial Information; (iii) aiding, agreeing, and conspiring with the Third Parties to intercept communications sent and received by Plaintiffs and Class Members; (iv) failing to obtain the written consent of Plaintiffs and Class Members to disclose their Personal and Financial Information to Third Parties for Third Party and fourth party use; (v) failing to protect Personal and Financial Information and take steps

to block the transmission of Plaintiffs' and Class Members' Personal and Financial Information through the use of tracking technology; (vi) failing to warn Plaintiffs and Class Members; and (vii) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of its customers' Personal and Financial Information.

15. Plaintiffs seek to remedy these harms and brings causes of action of (I) Negligence; (II) Negligence Per Se; (III) Invasion Of Privacy Cal. Const. Art. 1 § 1; (IV) Violation Of The Comprehensive Computer Data Access And Fraud Act ("CDAFA"), Cal. Penal Code § 502; (V) Violation Of California's Consumer Protection Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, *et seq*.; (VI) Violation of California Consumer Privacy Act ("CCPA"), 1798.100, *et seq*.; (VII) Violation of The California Customer Records Act ("CRA"), Cal. Civ. Code § 1798.80, *et seq*.; (VIII) Breach Of Implied Contract; (IX) Unjust Enrichment; (X) Bailment; (XI) Declaratory Judgment; (XII) Breach Of Confidence; (XIII) Violation of The California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 630, *et seq*.; (XIV) Violation of The Electronic Communications Privacy Act ("ECPA") 18 U.S.C. §§ 2511(1), *et seq*.; (XV) Violation of The Electronic Communications Privacy Act ("ECPA") 18 U.S.C. § 2511(3)(a) Unauthorized Divulgence By Electronic Communications Service; (XVI) Violation Of Title II Of The Electronic Communications Privacy Act ("Stored Communications Act") 18 U.S.C. § 2702, *et seq*.; (XVII) Violation of The Computer Fraud And Abuse Act ("CFAA") 18 U.S.C. § 1030, *et seq*..

16. Plaintiffs bring this action, individually and on behalf of all others similarly situated, for damages and equitable relief.

## PARTIES

17. Plaintiff Vishal Shah is a natural person and citizen of California, where he intends to remain, who resides in Buena Park, California in Orange County. Plaintiff Shah has been Capital

One's customer since February 2023 and is a victim of Defendant's unauthorized Disclosure of Personal and Financial Information.

18. Plaintiff Devin Rose is a natural person citizen of California, where he intends to remain, who resides in California. Plaintiff Rose has been Capital One's customer since March 2024 and is a victim of Defendant's unauthorized Disclosure of Personal and Financial Information.

19. Plaintiff Gary Ingraham is a natural person and citizen of California, where he intends to remain, who resides in Corning, California in Tehama County. Plaintiff Ingraham was Capital One's customer in April 2024 and is a victim of Defendant's unauthorized Disclosure of Personal and Financial Information.

20. Plaintiff Deia Williams is a natural person and citizen of California, where she intends to remain, who resides in Belmont, California. Plaintiff William was Capital One's customer in 2023 and is a victim of Defendant's unauthorized Disclosure of Personal and Financial Information.

21. Defendant Capital One is a stock corporation organized and existing under the laws of the State of Virginia, with a principal place of business located at 1680 Capital One Dr, Mc Lean, VA, 22102 - 3407, USA.[5]

22. Capital One's Registered Agent for Service of Process is Corporation Service Company, 100 Shockoe Slip Fl 2, Richmond, VA, 23219 - 4100, USA.[6]

[5] *See Capital One Financial Corporation*, Virginia State Corporation Commission Clerk's Information System, Entity Information, available at https://cis.scc.virginia.gov/EntitySearch/BusinessInformation?businessId=228610&source=FromEntityResult&isSeries%20=%20false (last visited Aug. 8, 2024).

[6] *Id.*

23. Capital One is a financial institution, as that term is defined by Section 509(3)(A) of the GLBA, 15 U.S.C. § 6809(3)(A).

24. Capital One has corporate offices in San Francisco, California,[7] and maintains at least twelve physical locations in the state of California.[8]

## JURISDICTION AND VENUE

25. This Court has personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business in this State in at least twelve different physical locations; it maintains corporate offices in California; and committed tortious acts in this State.

26. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than one hundred (100) members in the proposed Classes, and at least one member of the Classes is a citizen of a state different from Defendant.

27. This Court also has subject matter jurisdiction under 28 U.S.C. § 1331 because it arises under the laws of the United States.The Court has supplemental jurisdiction over Plaintiffs' claims arising under state law pursuant to 28 U.S.C. § 1367.

28. Venue is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events and omissions giving rise to Plaintiffs' claims occurred in this district and continue to occur in this district.

[7] *Corporate Offices*, CapitalOne.com, https://www.CapitalOne.com/about/corporate-information/corporate-offices (last visited Aug. 12, 2024).

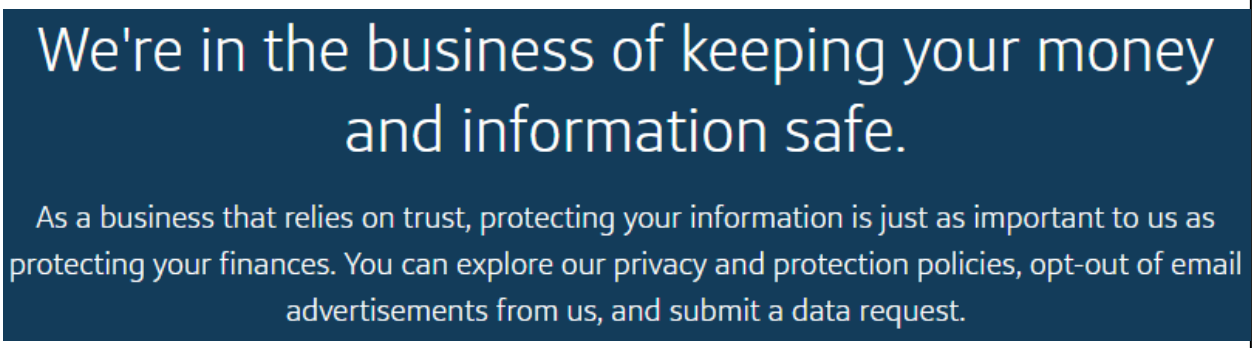
[8] *Capital One Café–Where Banking Meets Living*, CapitalOne.com, https://www.CapitalOne.com/local/#locations (last visited Aug. 12, 2024).

## COMMON FACTUAL ALLEGATIONS

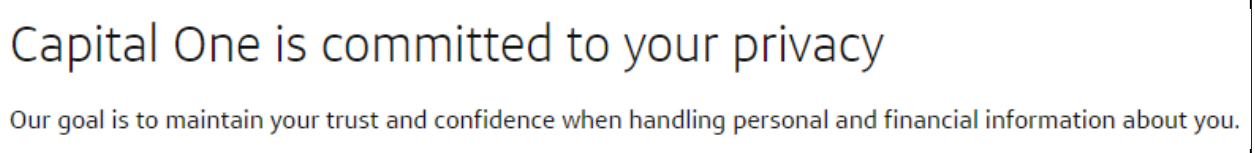
### A. Capital One: A Financial Powerhouse That Collects Personal and Financial Information Under the Guise of Protecting it

29. Capital One services "banking customer accounts through digital channels and [its] network" of physical locations.[9] As "one of the nation's largest banks" and the "third largest issuer of Visa and MasterCard credit cards in the United States,"[10] Capital One proclaims it is "in the business of keeping your money and information safe."[11]

30. Capital One represents to Customers:[12]




31. Capital One portrays its commitment to privacy to its Customers:[13]




32. On information and belief, Capital One provides financial services to Customers in every state in America.[14]

---

[9] *See Capital One's Annual Report for the 2023 Fiscal Year*, available at https://www.investor.Capital One.com/node/55906/html (last visited Aug. 7, 2024) ("*2023 Annual Report*"), p. 4.

[10] *Id.*

[11] *See U.S. Consumer Privacy Notice*, CapitalOne.com, https://www.capitalone.com/privacy/ (last visited Aug 8, 2024).

[12] *Id.*

[13] *Id.*

[14] *See, e.g., Locations*, CapitalOne.com, https://locations.capitalone.com/ (last visited Aug. 8, 2024).

33. In fact, as Capital One describes, it "operate[s] as an online direct bank in the United States."[15] Furthermore, in addition to being one of the largest issuers of "credit cards in the U.S. . . . we also offer debit cards, bank lending, treasury management and depository services, auto loans and other consumer lending products in markets across the U.S."[16]

34. "As one of the nation's largest banks based on deposits as of December 31, 2023," Defendant "service[s] banking customer accounts through digital channels and our network of branch locations, cafés, call centers and automated teller machines ('ATMs')."[17]

35. As of August 2024, Capital One offers 31 credit cards, including the Venture and Venture X cards.[18] For a Customer's use of the Venture X Rewards Credit Card, Capital One charges $395 annually.[19]

36. Defendant has "spent a decade building a full-service, digital-first national retail bank."[20] To this end, Defendant serves its Customers via its Website and encourages customers to use its Website to, for example, learn about Capital One and its credit cards and other services,[21] view educational financial resources,[22] check eligibility for credit cards,[23] compare Capital One's

[15] *See 2023 Annual Report*, p. 36.
[16] *Id.*, p. 4.
[17] *Id.*, p. 4.
[18] *See Compare Credit Cards & Apply*, CapitalOne.com, https://www.capitalone.com/credit-cards/compare/ (last visited Aug 8, 2024) ("*Compare Credit Cards*").
[19] *Id.*
[20] *Id.* p. 3.
[21] *See generally*, the Website.
[22] *See Learn and Grow*, CapitalOne.com, https://www.capitalone.com/learn-grow/ (last visited Aug. 8, 2024).
[23] *See Credit Cards*, CapitalOne.com, https://www.capitalone.com/credit-cards/ (last visited Aug 8, 2024) ("*Credit Cards*").

credit card offers,[24] "[s]ee if you're pre-approved for card offers,"[25] apply for credit cards,[26] activate a credit card,[27] enroll in online banking,[28] access credit card account and information,[29] manage credit card accounts,[30] manage credit card payments,[31] pay credit card bills,[32] and much more.[33]

37. In short, Defendant encourages customers to use its "full-service" Website to access "almost everything customers can get in a traditional bank branch."[34]

38. Defendant promotes the comprehensive functionality and use of its Website in service of its own goal of increasing profitability. In furtherance of that goal, Defendant purposely and secretly installed the Third Parties' online tracking technology onto its Website to gather information about Customers.

39. Capital One utilized the information it collected to market its services and bolster its profits by surreptitiously diverting the information to Third Parties like Facebook.

40. But Defendant did not only collect information for its own use; Capital One also shared—and continues to share—Customers' information, including Personal and Financial

---

[24] *See Compare Credit Cards*.

[25] *See Get Pre-Approved for a Capital One Credit Card*, CapitalOne.com, https://www.capitalone.com/credit-cards/preapprove/ (last visited Aug. 8, 2024) ("*Get Pre-Approved*").

[26] *See Credit Cards*.

[27] *See Sign in Page*, CapitalOne.com, https://verified.capitalone.com/auth/primer?exp=card (last visited Aug. 8, 2024) ("*Sign in Page*").

[28] *See Capital One Help Center*, CapitalOne.com, https://www.capitalone.com/help-center/credit-cards/?oC=CO5ed2SUs1 (last visited Aug. 8, 2024) ("*Help Center*").

[29] *Id.*

[30] *See Sign in Page.*

[31] *See How to Manage Your Credit Card Payments*, CapitalOne.com, https://www.capitalone.com/help-center/credit-cards/manage-your-credit-card-payments/ (last visited Aug. 8, 2024).

[32] *Id.*

[33] *See generally* the Website.

[34] *See 2023 Annual Report*, p. 3.

Information, with the unauthorized Third Parties who then use it for their own benefit and to benefit fourth parties who are even further removed from the Customers.

**B. Third Parties and Trackers: Collectors and Profiteers of Personal and Financial Information**

41. The invisible Third Party online tracking technologies installed by Capital One on its Website gathers a vast assortment of Customer data. The installation of these trackers—and thus their transmission of data—is in Capital One's exclusive control.

42. When an individual accesses a webpage containing online tracking technology from a Third Party, the trackers instantaneously and surreptitiously duplicate communications with that webpage and send them to the Third Party. The information travels directly from both the user's browser and the webpage owner's server and then on to the Third Party's server, based off instructions from the Third Party's tracker. The communications and information transmitted via these trackers are entirely in Defendant's control; Customers trust Capital One with the information they input on Capital One's Website, and Capital One is in complete and exclusive control of its Website and the data input therein. The transmission of Customers' data only occurs on webpages that contain tracking technology.

43. Online tracking technologies may not be deleted from an individual's device; they are built into a webpage, and a webpage user has no control or warning over their presence or data collection. Third party trackers cause information to flow directly from the website user's browser and the website owner's server to the Third Party itself. A webpage user cannot prevent or even detect this transmission of data.

44. Accordingly, without any knowledge, authorization, or action by a user, a website owner who has installed Third Party trackers is utilizing website source code to commandeer its

users' computing devices and web browsers, causing them to invisibly re-direct the users' communications to Third Parties.

45. In this case, Defendant employed the Third Party trackers to intercept, duplicate, and re-direct Plaintiffs' and Class Members' Personal and Financial Information to the Third Parties contemporaneously, invisibly, and without the customer's knowledge.

46. Consequently, when Plaintiffs and Class Members visited Defendant's Websites and communicated their Personal and Financial Information, that information was simultaneously intercepted and transmitted to the Third Parties.

47. The Third Party trackers do not provide any substantive content on Capital One's Website. Rather, their only purpose is to collect information to be used for the Third Party and fourth parties' marketing and sales purposes.

48. The Facebook or Meta Pixel, for example, "tracks the people and type of actions they take" on a website.[35] It can be used to gather customer data, identify customers and potential customers, target advertisements to those individuals, and market products and services. This includes when a user visits a particular webpage, clicks a button, fills out a form (including the information from the form like employment information, citizenship, etcetera), IP addresses, web browser information, page location, any custom events set by the website owner, the tracker ID, and more.[36] Facebook does all of this by using the Meta Pixel to send "events" to its server.

[35] *Retargeting*, Meta, https://www.facebook.com/business/goals/retargeting (last visited Aug. 11, 2024).

[36] *See, e.g.*, *Meta Pixel*, Meta for Developers, https://developers.facebook.com/docs/meta-pixel/ (last visited Aug. 11, 2024); *Specifications for Facebook Pixel Standard Events*, Meta, https://www.facebook.com/business/help/402791146561655 (last visited Aug. 11, 2024); *see also Facebook Pixel, Accurate Event Tracking, Advanced*, Meta for Developers https://developers.facebook.com/docs/facebook-pixel/advanced/ (last visited Aug. 11, 2024).

49. Once the data is collected via the Meta Pixel, Facebook aggregates it to build its own massive, proprietary dataset, which Facebook then uses to find new customers, drive sales, and understand ad impact. This is all to the benefit of the website owner, like Capital One, Facebook as the third party, and other fourth parties, all of whom use the information for targeted marketing campaigns. Targeting works by allowing fourth parties to direct their ads at particular "Audiences," subsets of individuals who, according to Facebook, are the "people most likely to respond to your ad."[37]

50. Data harvesting is big business for Facebook; it drives Facebook's advertising sales, which are its profit center. In 2023, Facebook generated nearly $135 billion in revenue, roughly 98% of which was derived in advertising revenue alone space.[38] This business model is not limited to Facebook. Data harvesting one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 were as high as $434 per user, for a total of more than $200 billion industry wide.

51. On information and belief, the trackers Defendant installed from other Third Parties, including Google, Microsoft, DoubleClick, New Relic, Adobe, Everest, Skai/Kenshoo, Snowplow, BioCatch, and Tealium, work similarly to the Meta Pixel and likewise transmitted Plaintiffs' and the Class Members' Personal and Financial Information without Plaintiffs' and Class Members' knowledge or authorization.

---

[37] *Audience Ad Targeting,* Meta, https://www.facebook.com/business/ads/ad-targeting (last visited Aug. 14, 2023).

[38] *Meta Reports Fourth Quarter and Full Year 2023 Results,* Facebook https://investor.fb.com/investor-news/press-release-details/2024/Meta-Reports-Fourth-Quarter-and-Full-Year-2023-Results-Initiates-Quarterly-Dividend/default.aspx (last visited Aug. 8, 2024).

52. The Google trackers allow Defendant to track and share with Google (1) who uses Capital One's website; (2) what is performed on the website; (3) when users visit the website; (4) where on the website users perform these actions; and (5) how users navigate through the website to perform these actions. Google gathers this information using trackers embedded on Capital One's Website and generates corresponding reports.[39] DoubleClick is part of the suite Google uses to collect all of this.[40] Google's collection of this data "enables advertisers to more effectively create, manage and grow high-impact digital marketing campaigns."[41]

53. The Microsoft tracker allows Defendant to "[t]rack what your customers are doing after they click on your ad."[42] According to Microsoft, the tracker "records what customers do on your website . . . [and] will collect data that allows you to track conversion goals and target audiences with remarketing lists."[43]

54. The New Relic tracker is an application performance management tool, used for application monitoring, which can track every action a user performs on the website.[44]

55. The Adobe tracker can collect a veritable wealth on information on Defendant's Website, including page views, clicks, time on page, scroll depth, video views, form submissions,

---

[39] *See generally, A big list of what Google Analytics can & cannot do,* MarketLyrics, avail. at https://marketlytics.com/blog/list-of-things-google-analytics-can-and-cannot-do/.

[40] *See the DoubleClick Digital marketing Suite,* Google Developers, https://developers.google.com/app-conversion-tracking/third-party-trackers/doubleclick (last visited Aug. 8, 2024).

[41] *See DoubleClick Digital Marketing,* Google Help, https://support.google.com/faqs/answer/2727482?hl=en (last visited June 26, 2024).

[42] *Microsoft Advertising,* Microsoft.com, https://about.ads.microsoft.com/en/tools/performance/conversion-tracking#:~:text=Universal%20Event%20Tracking%20(UET)%20is,target%20audiences%20with%20remarketing%20lists (last visited June 26, 2024).

[43] *Id.*

[44] *Monitor, Debug and Improve Your Entire Stack,* New Relic, https://newrelic.com/(last visited Aug. 8, 2024)

user demographics and interests, social media interactions, email subscriptions, purchases, search behavior, custom data (collected directly from the website, like customer IDs, email addresses, and purchase history), and other third-party data.[45] Everest Technologies is associated with Adobe Ads in collecting this information.[46]

56. The Skai/Kenshoo tracker can collect ad performance metrics like clicks, impressions, click-through rates, conversions, search terms, search volume, audience data, engagement metrics, and user behavior.[47]

57. Snowplow is a data collection platform that allows collection and management of a wide variety of data, and allows for the creations of "rich, unified customer profiles with out-of-the box identity resolution."[48]

58. The BioCatch tracker "[m]onitor[s] web and mobile banking sessions,"[49] in order to "get[] to know [customers], their idiosyncrasies, their digital habits – the when, how, where, and why they bank."[50] "Session activities, decisions, location, movements, timing, and more are parsed, matched, and coalesced continuously in real time."[51]

[45] *See Audience Manager Benefits*, Adobe, https://business.adobe.com/products/audience-manager/benefits.html (last visited Aug. 8, 2024)

[46] *See Our Services*, Everest, https://www.everesttech.com/services/?c=us (last visited Aug. 8, 2024); *Everest for Adobe,* Adobe, https://exchange.adobe.com/apps/ec/108141/everest-for-adobe (last visited Aug. 8, 2024).

[47] *See Omnichannel Marketing Platform,* Skai, https://skai.io/(last visited Aug. 8, 2024).

[48] *See Snowplow main page*, https://snowplow.io/ (last visited Aug. 8, 2024).

[49] *See Behavioral Biometrics*, https://www.biocatch.com/ (last visited Aug. 8, 2024).

[50] *See Why BioCatch,* https://www.biocatch.com/why-biocatch (last visited Aug. 8, 2024).

[51] *See Continuous Behavioral Sequencing*, https://www.biocatch.com/biocatch-connect/continuous-behavioral-sequencing (last visited Aug. 8, 2024).

59. The Tealium tracker can track page views, clicks, scroll depth, form submissions, video views, custom events, user information, marketing and sales data, and custom and third-party data.[52]

### C. Capital One Used Trackers to Unauthorizedly Disclose Personal and Financial Information

60. On information and belief, Capital One installed each of these trackers, through which Capital One transmitted Customers' communications with Capital One's website and thus their Personal and Financial Information to the Third Parties without Customers' knowledge or authorization. This information included their browsing activities including the pages they viewed and the buttons they clicked; information revealed in the application process regarding (i) their employment, (ii) bank accounts, and (iii) Customers' eligibility, pre-approval, or approval for a credit card; as well identifying information, such as IP addresses and identifying cookies.

61. On information and belief, since at least November 30, 2023, and at least as recently as June 24, 2024, Capital One has tracking technologies installed on its Website. Archives also show that Capital One previously configured Meta to pull information automatically from Capital One's Website.

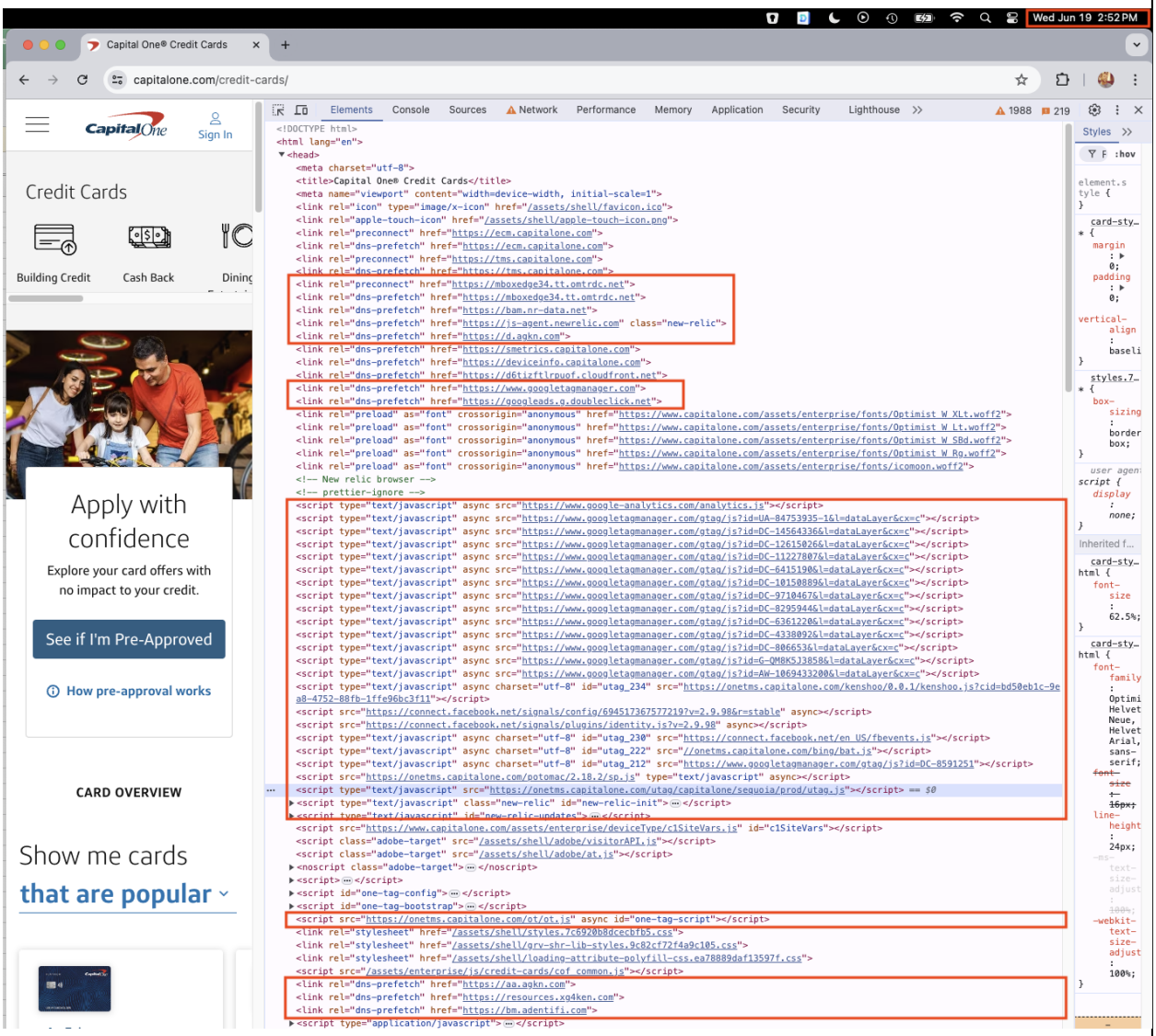
62. Accordingly, Capital One disclosed its Customers'—including Plaintiffs' and the Class Members'—data and Personal and Financial Information to the Third Parties, like Facebook, beginning some time prior to November 30, 2023, and at least up to June 24, 2024.

63. By way of example, as configured as of November 30, 2023, Defendant's Facebook Pixel and/or its other tracking technologies, disclosed significant information to Facebook.

[52] *See Customer Data Platform*, Tealium, https://tealium.com/ (last visited Aug. 8, 2024).

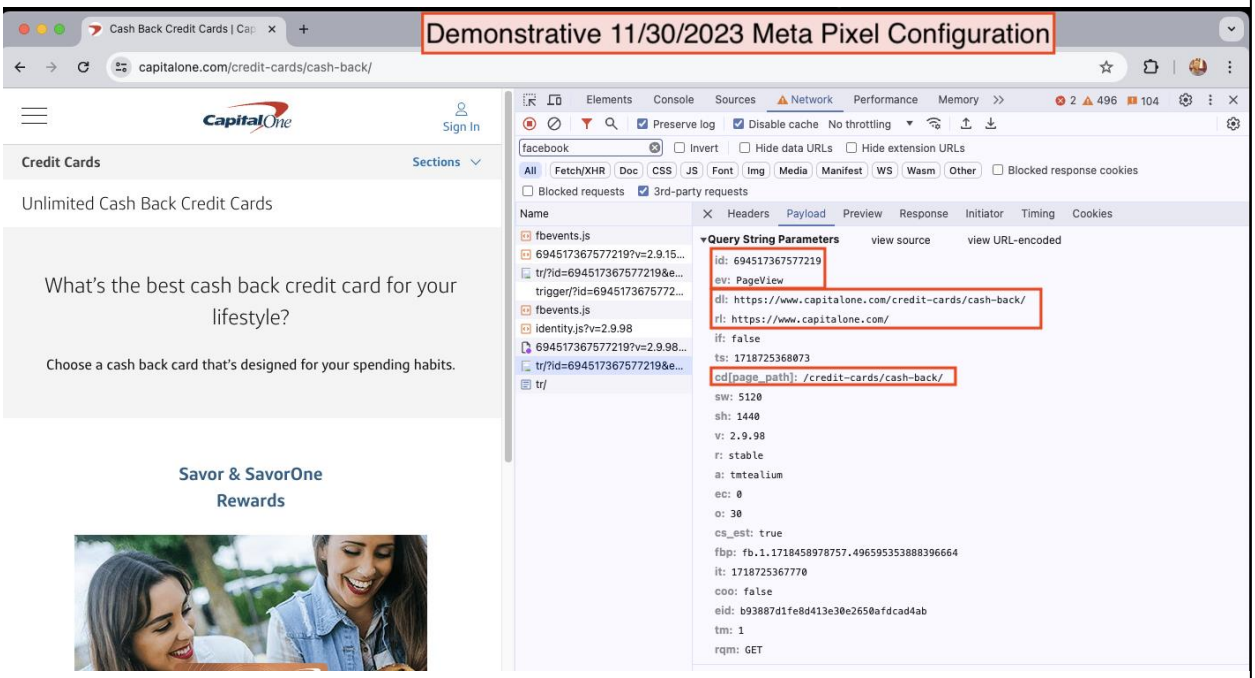
*i. Capital One Installed Meta Pixels to Track Customers' Browsing Activities Across its Website.*

64. Capital One configured the Facebook Events tracker to load a Meta Pixel with ID 694517367577219 ("Pixel1"):




65. Through Meta Pixel events, Capital One disclosed details about users' interactions with Capital One's Website as users applied for credit cards. For example, if a user clicked to learn about cashback credit cards, Capital One would send 'events' to Facebook as soon as the page

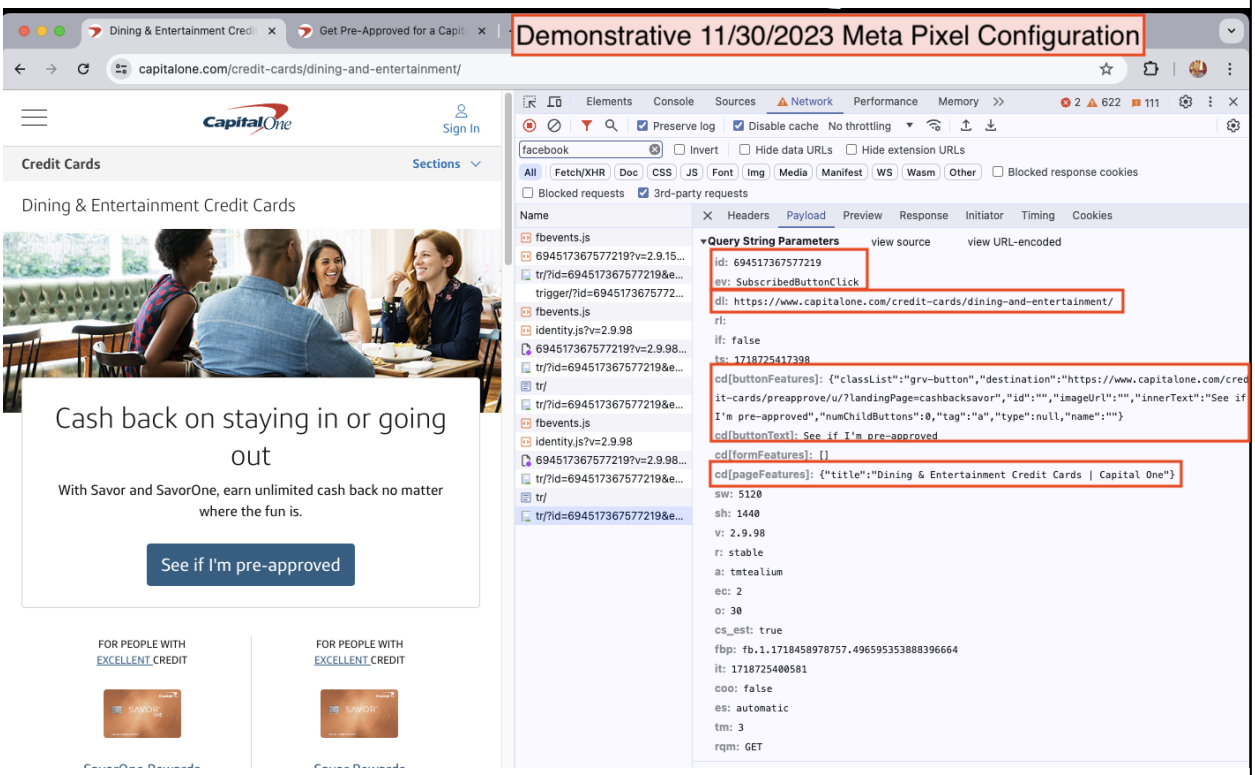
loaded, informing Facebook that the user was learning about "Cash Back Credit Cards | Capital One":




66. Then, if the user clicked to learn about credit cards that provide cash back on dining and entertainment, Capital One would send an event via the tracker informing Facebook of this activity.

67. As customers booked appointments on Capital One's website, Capital One would send Facebook events disclosing the customers' activities. The event would disclose that the user clicked a button labeled "See Cards" that led to the "credit-cards/dining-and-entertainment/" page. Capital One would then transmit events confirming that the user was exploring "dining & entertainment cash back credit cards from Capital One."

68. If the user then clicked to "See if I'm pre-approved," Capital One would send an event informing Facebook about the user's activity. The event reveals that the user clicked to go to "credit-cards/preapprove/u/?landingPage=cashbacksavor" to apply for pre-approval.




69. As users navigated through the pre-approval application process, Capital One continued to send details to Facebook about the users. The pre-approval application is a multi-page form. This type of form breaks down the data collection process into multiple steps or pages, each focusing on a specific section or set of questions. Once each step is completed, the user would need to click a "next" button to move on to the next step. Each time a user clicked the next button, Capital One would send an event to Facebook, with the event describing the form that the user was filling out.

70. During this process, Capital One sends Facebook information including, at a minimum, applicants' (i) employment, (ii) bank accounts, and (iii) Customers' eligibility, pre-approval, or approval for a credit card.

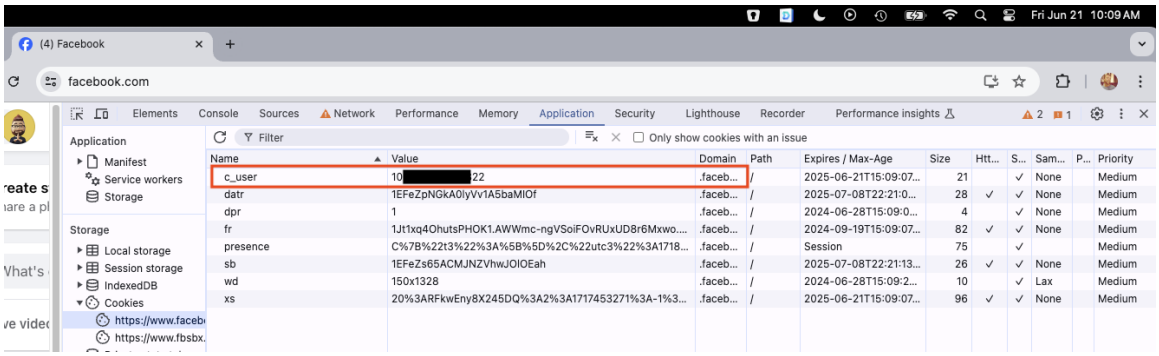
71. Furthermore, in each of the Meta Pixel events that Capital One sends to Facebook, Capital One includes a cookie which Facebook uses to identify users. Facebook can therefore

connect cookie data that Capital One transmits with specific users. Furthermore, Facebook's "Your activity off Meta technologies" report confirms that Facebook receives the data Capital One shares with Facebook.

*ii. Capital One Disclosed Customers' Identifying Information*

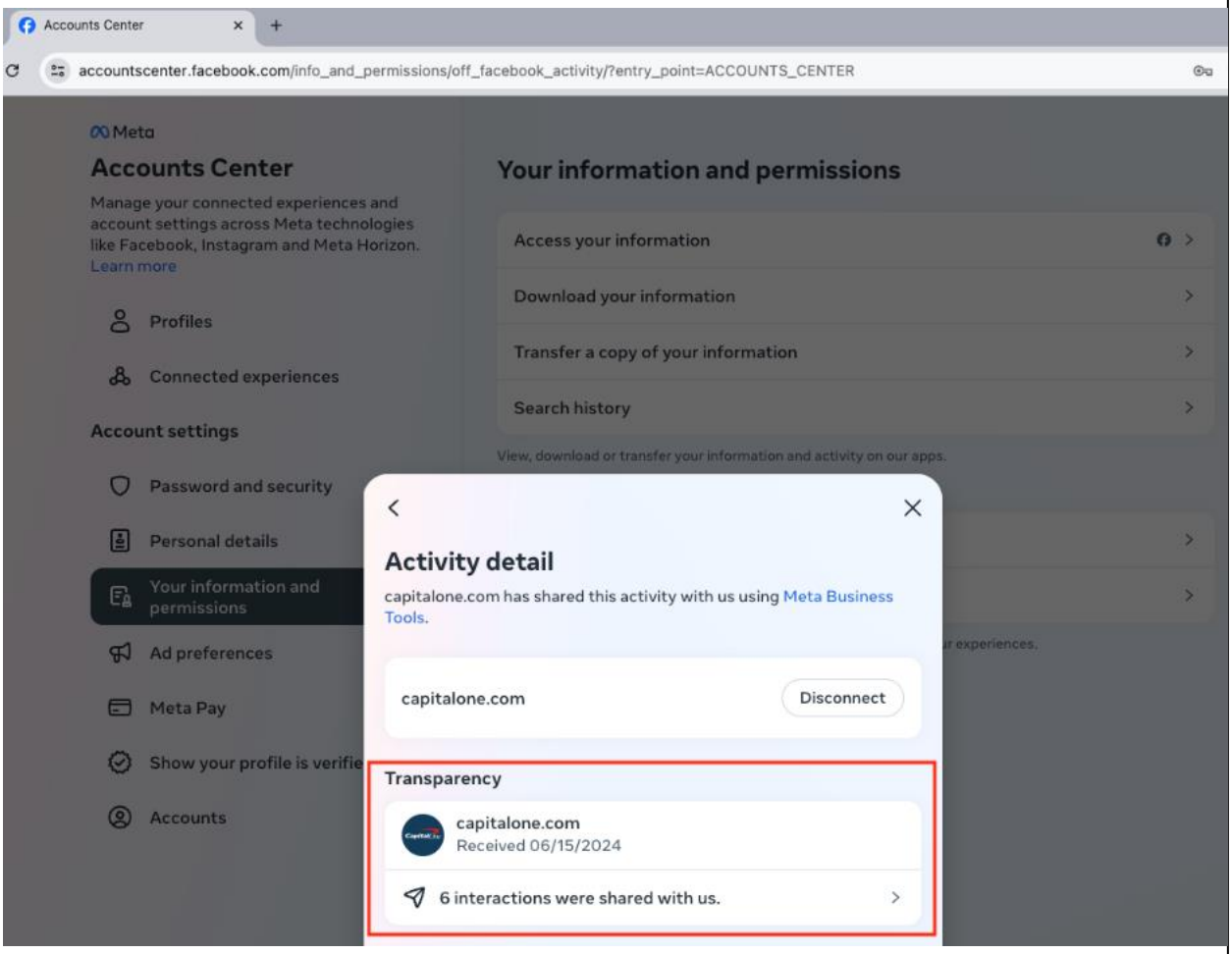
72. Defendant also disclosed Customers' identifying information, including their IP addresses and identifying cookies, and/or Facebook ID.

73. In each of the Facebook events that Capital One sent to Facebook, Defendant included a cookie which Facebook uses to identify users.




74. Facebook can therefore connect cookie data that Capital One transmitted with specific customers.

75. Furthermore, Facebook's "Your activity off Facebook technologies" report can confirm that Facebook received the data Capital One shared with Facebook.




76. Capital One transmits to Facebook the specific page viewed by the customer to Facebook, alongside the customer's IP address, individually identifying cookies, and/or the customer's unique Facebook ID. Thus, the pages customers viewed, alongside Personal and Financial Information inputted and disclosed therein, and further alongside identifying information, is reported back to Facebook, thereby revealing the customer's identity and Personal and Financial Information.

### D. Capital One Maintains Ambiguous, Disingenuous, and Deceptive Privacy Policies That Fail to Sufficiently Disclose, Notify, Or Provide Opportunity to Opt-Out of the Disclosure

77. Customers never consented, agreed, authorized, or otherwise permitted Defendant to intercept their Personal and Financial Information or to use or disclose it for marketing and

profit purposes. Customers were never provided with any written notice that Defendant disclosed their Personal and Financial Information to Third Parties (who then allowed fourth parties to use it for profit), nor were they provided means of opting out of such disclosures.

78. Customers relied on Defendant to keep their Personal and Financial Information confidential and securely maintained and to use this information only for the purpose of providing legitimate financial services. Customers relied on Defendant to make only authorized disclosures of this information.

79. Furthermore, Defendant actively misrepresented it would preserve the security and privacy of Customers' Personal and Financial Information.

80. The contracts that Capital One has with its Customers include "Our Privacy Protections",[53] "Online Privacy Policy,"[54] "U.S. Consumer Privacy Notice,"[55] "Manage Your Data",[56] "California Consumer Privacy Act Disclosure,"[57] and "Social Security Number Protections,"[58] (collectively, "Privacy Contracts").

81. "The Capital One Online Privacy Policy includes information for everyone about [Capital One's] online information practices."[59] Capital One promises that it is "in the business of

[53] *Our Privacy Protections*, https://www.capitalone.com/privacy/ (last visited Aug. 13, 2024) (Exhibit A).

[54] *Online Privacy Policy*, https://www.capitalone.com/privacy/online-privacy-policy/ (last visited Aug. 13, 2024) (Exhibit B).

[55] *U.S. Consumer Privacy Notice*, https://www.capitalone.com/privacy/notice/ (last visited Aug. 13, 2022) (Exhibit C).

[56] *Manage Your Data*, Capital One, https://mydata.capitalone.com/ (last visited Aug. 13, 2024) (Exhibit D).

[57] *California Consumer Privacy Act Disclosure*, https://www.capitalone.com/privacy/ccpa-disclosure/ (Exhibit E).

[58] *Social Security Number Protections*, https://www.capitalone.com/privacy/social-security-number/ (Exhibit F).

[59] *Our Privacy Protections* (Exhibit A).

keeping your money and information safe."[60] But Capital One fails to keep Customers' information safe, instead disclosing it to Third Parties (and eventually fourth parties) uninvolved in providing financial services to Plaintiffs and Class Members without Customers' authorization or consent.

82. "As a business that relies on trust, protecting your information is just as important to us as protecting your finances," Capital One tells Customers.[61] But despite recognizing its elevated position as trusted provider of financial services, Capital One fails to live up to that expectation by failing to protect the privacy of its Customers' information.

*i. The U.S. Consumer Privacy Notice*

83. "The U.S. Consumer Privacy Notice applies to customers, applicants, and former customers of the Capital One family of companies listed in the notice."[62] "It details [Capital One's] privacy and security practices regarding [its] relationship with [Customers] and provides instructions on how to limit the sharing of [Customers'] information."[63]

84. This notice recognizes that, under federal law, Customers may limit "sharing for nonaffiliates to market to" them.[64] Capital One's U.S. Consumer Privacy Notice represents:

> Federal law also requires us to tell you how we collect, share, and protect your personal . . . The types of personal information we collect and share depend on the product or service you have with us. This information can include:
> - Social Security number and income
> - Account balances and payment history
> - Account transactions and credit card or other debt[65]

85. But the types of personal information that Capital One collects and shares does ***not*** depend on the product or service a Customer has with it. Instead, Capital One indiscriminately

---

[60] *Id.*
[61] *Id.*
[62] *Id.*
[63] *Id.*
[64] *U.S. Consumer Privacy Notice* (Exhibit C).
[65] *Id.*

collects and shares Customer information without regard to the product or service a Customer has with Capital One.

86. Capital One "list[s] the reasons financial companies can share their customers' personal information; the reasons Capital One chooses to share; and whether you can limit this sharing."[66] Those reasons include "our everyday business purposes-such as to process your transactions, maintain your accounts(s), respond to court orders and legal investigations, or report to credit bureaus"; "For our marketing purposes – to offer our products and services to you"; "For joint marketing with other financial companies"; "For our affiliates' everyday business purposes – information about your transactions and experiences"; "For our affiliates' everyday business purposes – information about your creditworthiness"; "For our affiliates to market to you"; and "For our nonaffiliates to market to you."[67]

87. The U.S. Consumer Privacy Notice defines an Affiliate as "Companies related by common ownership or control. They can be financial and nonfinancial companies."[68] Joint marketing is "A formal agreement between nonaffiliated financial companies that together market financial products or services to [Customers]."[69] Capital One's "joint marketing partners include companies such as other banks and insurance companies."[70] Certainly, Third Parties like Facebook do not meet either of these definitions. Capital One finally defines "nonaffiliates," which are "Companies not related by common ownership or control."[71] "They can be financial and nonfinancial companies."[72] Capital One identifies the types of "[n]onaffiliates we share with"

[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] *Id.*

which "***can include*** insurance companies, co-branded partners, retailers, data processors, and advertisers."[73] It is not clear that the Third Parties fall under this category—Facebook, for example, is a social media company, not an insurance company, co-branded partner, retailer, data processor, or advertiser.[74]

88. In stating that it "can include" its Customers' Personal and Financial Information, the U.S. Consumer Privacy Notice grants Capital One the sole discretion to determine whether it will share Customers' information with nonaffiliates. It does not include any information explaining or specifying what information it shares with nonaffiliates or under what conditions and circumstances it may do so. Capital One thus maintains complete discretion on whether and what to disclose and when it discloses it.

89. Customers reasonably understand that Capital One will securely maintain their Personal and Financial Information entrusted to it and protect that information from being shared or utilized by Third Parties (and fourth parties) that have nothing to do with Capital One or its services. Capital One's U.S. Consumer Privacy Notice only reinforced this reasonable understanding.

90. Nevertheless, Capital One abuses the contractual discretion it reserved wholly for itself and acts in a manner that it knows to be inconsistent with its Customers' reasonable expectations under its U.S. Consumer Privacy Notice.

[73] *Id.*

[74] Like Capital One, Third Parties like Facebook may include advertisements on their platforms and websites, but that does not automatically make them an "advertiser." Advertising is not even the primary use of Third Parties or social media companies like Facebook.

91. By always exercising its discretion in its own favor and to the detriment of Customers, Defendant breaches the reasonable expectations of Customers and, in doing so, violates its duty to act in good faith.

*ii. The Online Privacy Policy*

92. Capital One also requires Customers using its Website to agree to the terms of its Online Privacy Policy.[75]

93. Capital One states in its Online Privacy Policy that it "may collect information" both directly from Customers and automatically when they use Capital One's Website.[76] The Privacy Policies explain:

> This Privacy Policy applies to information we collect when you use our Online Services. We may combine that information with information we collect in other contexts, such as from our phone calls and emails with you, from third-party data sources for fraud prevention, identity verification, or marketing purposes, from our co-branded card or business partners, and from publicly available data sources. We will treat such combined information in accordance with this Privacy Policy.[77]

94. Nowhere in the policies does Capital One disclose its use of Customer Personal and Financial Information for Third Party and fourth party marketing.

95. Capital One's Online Privacy Policy specifically enumerates the types of entities with which Capital One can share Customers' Personal and Financial Information. Such categories include: (1) affiliates; (2) business partners; (3) service partners; (4) third parties with whom Customers specifically authorize or direct Defendant to share their information, such as to "transfer funds to another bank"; (5) credit bureaus; and (6) government entities with whom Capital One shares information for legal or necessary purposes. [78] Facebook and the other Third Parties (and

[75] *See Online Privacy Policy* (Exhibit B).
[76] *Id.*
[77] *Id.*
[78] *Id.*

fourth parties) with which Capital One actually shares Customers' Personal and Financial Information do not fit into any of these categories.

96. The Online Privacy Policy provides a final, catch-all category, which permits Capital One to "share ***aggregated and de-identified information*** (such as aggregated statistics regarding the use of our financial products and services) with third parties for any purpose."[79]

97. The Online Privacy Policy thus makes clear that, if Capital One desires to share Customers' Personal and Financial Information with a Third Party like Facebook, such information cannot contain any details linking it to specific Customers. Rather, the information may be shared only in an "aggregated and de-identified" form.

98. Capital One violates this agreement by sharing Customers' Personal and Financial Information with Third Parties in a manner that is neither aggregated nor de-identified. To the contrary, Capital One routinely shares Customers' Personal and Financial Information in a format that enables the Third Parties to identify and target specific Customers.

99. Capital One's Online Privacy Policy also enumerates and exemplifies the purposes for which Capital One may use Customer information. Such purposes include:

> **Providing our products and services**, such as enabling you to apply for and obtain Capital One products or services, evaluating your application or eligibility for a Capital One product or service, servicing and managing your accounts, providing customer service or support, communicating with you, and providing online tools and features.
> **Processing transactions and payments**, such as transferring funds between accounts, processing payments or transactions, fulfilling orders, and conducting settlement, billing, processing, clearing, or reconciliation activities, and helping you book flights, hotels, events, and other reservations through our travel, entertainment, or dining services.
> **Verifying your identity**, such as conducting identity verification when you apply for our products or services, authenticating your login credentials, verifying your location to allow access to your accounts, and storing security questions for subsequent verification online or over the phone.

[79] *Id*. (emphasis added).

> **Detecting and preventing fraud**, such as determining fraud risk and identifying fraudulent transactions.
> **Protecting against security risks**, such as monitoring network activity logs, detecting security incidents, conducting data security investigations, and otherwise protecting against malicious, deceptive, fraudulent, or illegal activity.
> **Advertising and marketing**, such as sending you offers for special products and services via mail, email, or text message, displaying online advertising, targeting our offers or promotions, providing sweepstakes, conducting market research, and evaluating or improving the effectiveness of our marketing efforts. Learn more about how we use online tracking technology.
> **Conducting analytics and research**, such as examining which parts of our website you visit or which aspects of our mobile apps you find most useful, evaluating user interface and experiences, testing features or functionality, performing debugging and error repair, and analyzing the use of our Online Services. Learn more about how we use online tracking technology.
> **Improving our products and services**, such as personalizing and optimizing your website and mobile experiences, recognizing you across different browsers and devices you use, improving existing products and services, and developing new products and services.
> **Carrying out legal and business purposes**, such as complying with applicable laws, responding to civil, criminal, or regulatory lawsuits, subpoenas, or investigations, exercising our rights or defending against legal claims (including for collections and recoveries on past-due accounts), resolving complaints and disputes, performing compliance activities, analyzing credit risk, conducting credit reporting activities, regulatory reporting, performing institutional risk control, conducting human resources activities, and otherwise operating, managing, and maintaining our business.
> **Creating aggregated and de-identified information**, such as using or modifying the information described in this Privacy Policy in a manner that does not allow us to reasonably identify you. For example, we may compile aggregated statistics to understand trends or to research the percentage of users accessing a specific website feature. Information that has been aggregated and de-identified is no longer subject to this Privacy Policy.[80]

None of these authorized disclosures permit Capital One to share Customers' Personal and Financial Information for Third Party and fourth party marketing or targeted advertisement.

100. Furthermore, this language limits Capital One's disclosure to third-parties "acting on its behalf."[81] Thus, to the extent that sharing with Third Parties was permitted at all, marketing

[80] *Id.*
[81] *Id.*

is limited to advertisements for Capital One and its products and services—not Third Parties' and fourth parties' products or services.

101. Capital One again explains the groups with and context in which it "may" share this collected information:

> **Affiliates**. We may share information with companies in the Capital One family.
> **Business partners**. We may share information with companies that we have partnered with to offer or enhance products and services for Capital One customers or prospective customers. For example, we may share information with co-branded credit card partners, joint marketing partners, bill pay partners, or retail partners that allow you to redeem credit card rewards.
> **Marketing partners**. We may allow companies to collect information through our Online Services in order to provide marketing services to us, including to target advertising to you based on personal information collected across different websites, mobile apps, and devices over time. Learn more about how we use online tracking technology to conduct personalization, analytics, and targeted advertising, and how you can opt out.
> **Service providers**. We use other companies to provide services on our behalf and to help us run our business. We may share information with these service providers, or they may collect information on our behalf, for various business purposes. For example, we use service providers for hosting and securing our information systems, servicing customer accounts, detecting and preventing fraud, assisting with human resources activities, communicating with our customers, and analyzing and improving our Online Services.
> **Other third parties with your consent or as necessary to provide our products and services.** We share information with your consent or at your direction, such as when you ask us to share information with a money management app to track your financesor to share financing details with an auto dealer when shopping for a car. We also may share information with third parties to provide products and services that you request, such as with merchants that are authorizing Capital One credit card transactions, with travel, entertainment, or restaurant providers when you transfer funds or send money to friends and family via Zelle, and with third-party payment processors (such as Paypal or Stripe) when you make payment on our Online Services.
> **Credit bureaus.** We share information with credit reporting agencies, such as Experian, Transunion, and Equifax, to report on or learn about your financial history and for other lawful purposes.
> **Government entities and others with whom we share information for legal or necessary purposes.** We share information with government entities and others for legal and necessary purposes, such as:
>
> - To respond to requests from our regulators or to respond to a warrant, subpoena, governmental audit or investigation, law enforcement request, legal order, or other legal process.

- In connection with a proposed or actual sale, merger, transfer, acquisition [*sic*], bankruptcy, or other disposition of some or all of our assets, in which case we may share information with relevant third parties.
- For other legal purposes, such as to enforce our terms and conditions, exercise or defend legal claims, comply with applicable laws, or if we determine that disclosure is necessary or appropriate to protect the life, safety, or property of our customers, ourselves, or others.[82]

102. None of the entities or uses authorize disclosure of Customers' Personal and Financial Information to Third Parties for their use in Third Party and fourth party marketing and targeted advertisement.

103. Where Capital One's Online Privacy Policy does discuss marketing and advertisement, it makes clear that Customer information will be used only in relation to *Capital One's* own services and advertising. For example:

> [Capital One] may use information about you for the purposes [of]… Providing **our** products and services . . . Improving **our** products and services
> Capital One may customize content and advertisements for **our** products and services on our own and third-party websites and mobile apps…. We and our third-party providers use online tracking technologies to engage in data analytics, auditing, measurement, research, reporting, and debugging on **our** Online Services and to measure the effectiveness of **our** advertising. . . .[83]

104. No provision notifies Customers that Capital One discloses Customer Personal and Financial Information to Third Parties for Third Party and fourth party marketing and advertising use.

105. The Online Privacy Policy's only discussion of using pixels or cookies to conduct targeted advertising also fails to authorize Capital One's practice of sharing Customer information with Third Parties. That is because the Policy limits pixel or cookie activity that occurs "***on or through the Online Services***."[84]

---

[82] *Id.*
[83] *Id.* (emphasis added).
[84] *Id.* (emphasis added).

106. Third Party trackers are not "on or through the Online Services." That term is defined in the Online Privacy Policy to mean "***Capital One's*** websites, mobile applications, and other online services ***that link to this Privacy Policy***."[85] Third Party trackers and advertisements do not "link to this Privacy Policy" and are not "Online Services," which is confirmed by the Online Privacy Policy's warning that the policy "***does not apply*** to the websites, mobile applications, or other online services of . . . non-Capital One companies, such as our co-branded partners, auto dealerships and auto-finance companies, or any third-party websites that we link to online."[86]

107. Thus, the Online Privacy Policy's discussion of cookies or pixels does not apply to the collection or disclosure of information to Third Parties or their trackers for targeted advertising on their platforms (and fourth party platforms).

108. Capital One's disclosure of its use of "Pixel tags" further does not apply to the Third Parties because the Third Parties are not "service providers," as required in that provision.

109. The "Pixel tags" disclosure states:

> **Pixel tags**. A pixel tag (also known as a web beacon, clear GIF, pixel, or tag) is an image or a small string of code that may be placed in a website, advertisement, or email. It allows companies to set or read cookies or transfer information to their servers when you load a webpage or interact with online content. For example, ***we or our service providers*** may use pixel tags to determine whether you have interacted with a specific part of our website, viewed a particular advertisement, or opened a specific email.[87]

110. This language limits the entities that can use pixel tags to Capital One and its "service providers." The Online Privacy Policy defines a service provider as "other companies [that] provide services ***on our behalf and to help us run our business***…[T]hey may collect

[85] *Id.* (emphasis added).
[86] *Id.* (emphasis added).
[87] *Id.* (bolded italics added).

information ***on our behalf, for various business purposes***."[88] "For example, we use service providers for hosting and securing our information systems, servicing customer accounts, detecting and preventing fraud, assisting with human resources activities, communicating with our customers, and analyzing and improving our Online Services."[89] Third Party use of Customer data for Third Party and fourth party advertisement does not fall within these definitions and therefore is not permitted by the Online Privacy Policy.

111. Further, like the U.S. Consumer Privacy Notice, Capital One's Online Privacy Policy grants Capital One sole discretion to share Customers' Personal and Financial Information, stating: "We ***may*** share information in a variety of contexts."[90]

112. Customers reasonably understand that Capital One will securely maintain their Personal and Financial Information entrusted to it and protect the information from being shared or utilized by Third Parties (and fourth parties) that have nothing to do with Capital One or its services. Capital One's Online Privacy Policy only reinforced this reasonable understanding.

113. Nevertheless, Capital One abuses its contractual discretion it reserved wholly for itself and acts in a manner that it knows to be inconsistent with its Customers' reasonable expectations under its Online Privacy Policy.

114. By always exercising its discretion in its own favor and to the prejudice of Customers, Defendant breaches the reasonable expectations of Customers and, in doing so, violates its duty to act in good faith.

[88] *Id.* (emphasis added).
[89] *Id.*
[90] *Id.* (emphasis added).

*iii. The California Consumer Privacy Act Disclosure*

115. Capital One specifically promises California residents: "We will not share information we collect about you with nonaffiliated third parties, except as permitted by law, including, for example, with your consent or to service your account."[91]

116. The California Consumer Privacy Act Disclosure limits Capital One's ability to share information with "other third parties" to entities such as "[p]ayment processors, merchants, or other financial institutions" and, even then, sharing is limited to instances where Customers consent or "as necessary to provide ***our*** products and services."[92]

117. Capital One and its California Customers thus agreed that Capital One may share their Personal and Financial Information with nonaffiliated third parties only if the Customer expressly consented or, where "necessary," for the limited purpose of providing ***Capital One's*** products and services.

118. Instead of keeping the promises in its California Consumer Privacy Act Disclosure, Capital One indiscriminately shares Personal and Financial Information with nonaffiliated Third Parties, without Customers' consent and for Third Party and fourth party marketing purposes that have nothing to do Capital One servicing the Customer's account.

*iv. Capital One Does Not Permit Customers to Opt-Out of its Sharing with Third Parties.*

119. Capital One's failure to safeguard the privacy of Customers' Personal and Financial Information as agreed in its Privacy Policies is even more egregious here, as Capital One also fails to provide Customers with sufficient opportunity to opt out of disclosure to nonaffiliates (or any other party, for that matter). This is because, as described above, while the U.S. Consumer Privacy

[91] *U.S. Consumer Privacy Notice* (Exhibit C).
[92] *California Consumer Privacy Act Disclosure* (Exhibit E) (emphasis added).

Notice states that Customers may "limit this sharing," the Third Party trackers will still instantaneously send data from Customers that visit Capital One's Website ***even if*** a Customer calls the provided toll-free number and specifically requests that Capital One stop or otherwise limit the sharing of their Personal and Financial Information (i.e., after the Customer has 'opted out').

120. As Capital One's Online Privacy Policy explains, Customers can "opt out of certain targeted advertising" but "your preferences will apply only to the specific browser or device from which you opt out."[93] Customers are left with no way to fully opt out of Third Party disclosures and targeted advertising. In this way, Capital One not only fails to provide Customers with appropriate opportunity to opt out, but also fails to abide by its Customers' opt out requests as agreed in the U.S. Consumer Privacy Notice.

121. Capital One directs Customers to its "Google Analytics on our Online Services," and provides an "opt out" link.[94] But as discussed above, this both fails to provide Customers with actual opportunity to opt out, and fails to abide by the opt out request, since Third Party trackers will continue to instantaneously send data from Customers visiting Capital One's Website. Customers have **no** option to fully opt out.

122. Similarly, Capital One purports to allow Customers to "Manage [Thei]r Data."[95] Capital One tells Customers: "we use data to: Service your accounts and improve your experience[;] Personalize offers and services[;] Verify your identity to protect you from fraud[; and] Comply with state and federal regulations."[96] But Capital One offers limited options to

[93] *Online Privacy Policy* (Exhibit B).
[94] *Id.*
[95] *Manage Your Data* (Exhibit D).
[96] *Id.*

"manage your data"—Customers may download a copy of their data, request Capital One correct data, or request Capital One delete data.[97]

123. Again, these options do not sufficiently allow Customers to opt-out of Capital One's data collection and Disclosure through third party tracking technology. Furthermore, these promises are nothing but a sham; even when a Customer requests Capital One delete their data, in **949 out of 953** instances, Capital One finds a reason **not** to do so.[98] That equates to a 0.4% chance that Capital One **will** delete data when requested; inversely, there is a 99.6% chance that Capital One **will not** delete data when requested.[99]

124. Capital One's privacy policies as they were in place in January 2020 are substantially the same as they are now.[100]

**E. Capital One Violated the GLBA, FTC Standards, and Related Regulations**

125. As a financial institution, Capital One is subject to the GLBA. 15 U.S.C. § 6809(3)(A) (a "financial institution" is "any institution the business of which is engaging in financial activities..."). Defendant recognizes this, noting, "[f]or example, at the federal level, we are subject to the GLBA . . . among other laws and regulations . . . Additionally, the Federal Banking Agencies, as well as the SEC and related self-regulatory organizations, regularly issue

[97] *Id.*

[98] *2023 Transparency Report*, Capital One, https://mydata.capitalone.com/transparency-report (last visited Aug. 13, 2024).

[99] Numerically speaking, 4/953=0.004 or 0.4%; 949/953=.996 or 99.6%.

[100] *See Capital One U.S. English Privacy Opt Out Notice* (June 2020), CapitalOne.com, *available at* https://web.archive.org/web/20200620142711mp_/https://www.capitalone.com/privacy/notice/en-us/; *Capital One Online Privacy Policy* (Apr. 2020), CapitalOne.com, *available at* https://web.archive.org/web/20200421221756/https://www.capitalone.com/privacy/online-privacy-policy.

guidance regarding cybersecurity that is intended to enhance cyber risk management among financial institutions."[101]

126. Pursuant to the GLBA, "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801(a).

127. The FTC has interpreted Section 5 of the FTC Act, 15 U.S.C. § 45, to include compliance with the GLBA Privacy Rule, 16 C.F.R. § 313.1 *et seq*. The FTC consistently enforces the GLBA Privacy Rule, as failure to comply with the GLBA Privacy Rule is an unfair act or practice prohibited by Section 5 of the FTC Act.[102]

128. The GLBA Privacy Rule is a regulation that "governs the treatment of nonpublic personal information about consumers by the financial institutions." 16 C.F.R. § 313.1 *et seq*.

129. Pursuant to the GLBA Privacy Rule, "[a] financial institution must provide a notice of its privacy policies and practices with respect to both affiliated and nonaffiliated third parties, and allow the consumer to opt out of the disclosure of the consumer's nonpublic personal information to a nonaffiliated third party if the disclosure is outside of the exceptions."[103] Capital One consistently fails to do this.

130. The GLBA Privacy Rule, defines sensitive information that should not be indiscriminately disclosed:

> (n) (1) Nonpublic personal information means:
> (i) Personally identifiable financial information; and

---

[101] *See 2023 Annual Report*.

[102] *See How to Comply with the Privacy Rule*, https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act (last visited Aug. 22, 2024) ("The FTC may bring enforcement actions for violations of the Privacy Rule.").

[103] *See* FTC, *Financial Privacy Rule*, https://www.ftc.gov/legal-library/browse/rules/financial-privacy-rule (last visited August 8, 2024).

> (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.…
>
> (3) Examples of lists—
>
> (i) Nonpublic personal information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information (that is not publicly available), such as account numbers.…
>
> (o) (1) Personally identifiable financial information means any information:
>
> (i) A consumer provides to you to obtain a financial product or service from you;
>
> (ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or
>
> (iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.
>
> (2) Examples—
>
> (i) Information included. Personally identifiable financial information:
>
> (A) Information a consumer provides to you 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 your customers or has obtained a financial product or service from you;
>
> (D) Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;
>
> (E) Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a credit account;
>
> (F) Any information you collect through an Internet "cookie" (an information collecting device from a web server); and
>
> (G) Information from a consumer report.

16 C.F.R. § 313.3

131. The information that Capital One disclosed to Third Parties via trackers—including *e.g.*, information revealed in the application process regarding (i) their employment, (ii) bank accounts, and (iii) Customers' eligibility, pre-approval, or approval for a credit card; the users'

tracker ID (which identified to each Third Party that the user that was interacting with Capital One's financial services platform); the URL of the pages visited (which disclosed the financial services the user was obtaining); and the "clicks" the user made on Capital One's website (which is information Capital One obtained from the Customer in connection with providing financial products and services)—is "nonpublic personal information" under the GLBA and related regulations. 16 C.F.R. § 313.3.

132. Capital One has utterly failed to meet its privacy obligations under the GLBA: it has explicitly disclosed Customers' nonpublic personal information and Personal and Financial Information to Third Parties for marketing and advertisement, including for Third Party and fourth party advertising use, and refused to allow customers to meaningfully limit this sharing.[104]

133. Capital One fails to meet its notice obligations under the GLBA. "[A] financial institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information, unless such financial institution provides or has provided to the consumer a notice that complies with section 6803 of this title." 15 U.S.C.A. § 6802. As outlined at length above, Capital One's Privacy Policies fail to put Customers on notice as required here and actually promise that Customers' Personal and Financial Information will not be shared with Third Parties (and fourth parties) for targeted advertising purposes.

134. For example, by not including in its Privacy Policies that it discloses Customers' Personal and Financial Information to Third Parties for their use in their own advertising and marketing, the Privacy Policies fail to properly disclose:

> (1) the policies and practices of the institution with respect to disclosing nonpublic personal information to nonaffiliated third parties . . . including []the categories of persons to whom the information is or may be disclosed, other than the persons to whom the information may be provided [and] the policies and

[104] *U.S. Consumer Privacy Notice* (Exhibit C).

> practices of the institution with respect to disclosing of nonpublic personal information of persons who have ceased to be customers of the financial institution . . .
> (2) the categories of nonpublic personal information that are collected by the financial institution; [and]
> (3) the policies that the institution maintains to protect the confidentiality and security of nonpublic personal information

15. U.S.C.A. § 6803.

135. As detailed above, Capital One also fails to meet its opt out obligations under the GLBA. The GLBA Privacy Rule requires financial institutions to, for example, "provide an opt out notice" to Customers, which notice "must state…[t]hat the consumer has the right to opt out of that disclosure [and] [a] reasonable means by which the consumer may exercise the opt out right." 16 C.F.R. § 313.7. Under the GLBA, Capital One

> may not disclose nonpublic personal information to a nonaffiliated third party unless—
> (A) [it] clearly and conspicuously discloses to the consumer. . . that such information may be disclosed to such third party;
> (B) ***the consumer is given the opportunity***, before the time that such information is initially disclosed, ***to direct that such information not be disclosed to such third party***; and
> (C) the consumer is given an explanation of how the consumer can exercise that nondisclosure option.

15 U.S.C.A. § 6802 (emphasis added).

136. Capital One fails to meet its opt out obligations because, as outlined above in the Privacy Policies section, Capital One does not clearly and conspicuously disclose to Customers its Disclosure of their Personal and Financial Information to Third Parties.

137. Capital One further fails to meet its opt out obligations because Customers are not provided an opportunity before disclosure to direct the nondisclosure of their information—as described above, Capital One instantaneously discloses information when Customers visit its Website.

138. Capital One further fails to meet its opt out obligations because it does not provide Customers with an explanation of how they can exercise a nondisclosure option.

139. Capital One still further fails to meet its opt out obligations because it fails to provide Customers with reasonable means of opting out. The GLBA Privacy Rule provides "examples of reasonable opportunity to opt out":

> (i) By mail. You mail the notices required in paragraph (a)(1) of this section to the consumer and allow the consumer to opt out by mailing a form, calling a toll-free telephone number, or any other reasonable means within 30 days from the date you mailed the notices.
> (ii) By electronic means. A customer opens an on-line account with you and agrees to receive the notices required in paragraph (a)(1) of this section electronically, and you allow the customer to opt out by any reasonable means within 30 days after the date that the customer acknowledges receipt of the notices in conjunction with opening the account.
> (iii) Isolated transaction with consumer. For an isolated transaction, such as the purchase of a money order by a consumer, you provide the consumer with a reasonable opportunity to opt out if you provide the notices required in paragraph (a)(1) of this section at the time of the transaction and request that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction.

16 C.F.R. § 313.10.

140. The only targeted advertising opt out procedure Capital One provides Customers fails to meet this requirement because, to "[o]pt out of targeted advertising," Customers must enable settings in their own browser.[105] This is not "reasonable" as outlined in the GLBA Privacy Rule.

141. Capital One father fails to comply with its opt out obligations because it fails to fully abide by its Customers' opt out. When attempting to opt out of targeted advertising, Customers are left with an option that "will apply only to the specific browser or device from

[105] *Online Privacy Policy* (Exhibit B).

which you opt out."[106] Third Party trackers will continue to instantaneously send data from Customers visiting Capital One's Website. Customers have **no** option to fully opt out of Disclosures to Third Parties or targeted advertising.

142. Capital One further fails to comply with its opt out obligations by providing Customers with an "opt out" link for its use of "Google Analytics on our Online Service."[107] But as discussed above, this both fails to provide Customers with actual opportunity to opt out, and fails to abide by the opt out request, since Third Party trackers will continue to instantaneously send data from Customers visiting Capital One's Website. Customers have **no** option to fully opt out.

143. By perpetually disclosing its customers' Personal and Financial Information to third parties without consent, Capital One failed and continues to fail to meet its obligations under the GLBA, FTC standards, and related regulations, to establish appropriate standards and safeguards relative to Customers' Personal and Financial Information.

**F. Plaintiffs' Experiences**

144. Plaintiff Vishal Shah has a 360 Checking Account with Capital One.

145. Plaintiff Shah has been Defendant's customer since January 2020.

146. Plaintiff Shah further applied for Defendant's services on approximately January 24, 2023, when he applied for the Capital One Venture X credit card.

147. Plaintiff Shah pays approximately $395 annually to use his Venture X credit card.

148. During the last three years, Plaintiff Shah accessed his financial information maintained by Capital One through Capital One's Website.

[106] *Id.*
[107] *Id.*

149. Plaintiff Shah was approved for the Capital One Venture X credit card and has used the card at least in California since being approved.

150. Plaintiff Shah has used Capital One's Website to facilitate his financial services with Defendant since February 2023 and inputted Personal and Financial Information into Defendant's Website at Defendant's direction and encouragement. .

151. Plaintiff Shah used Capital One's Website to apply for a credit card.

152. Plaintiff Shah is a Facebook user, who joined Facebook within the last ten years.

153. Shortly after Plaintiff Shah used Defendant's Website to apply for his Capital One Venture X card, advertisements from NerdWallet, advertising random credit cards, began appearing in his Facebook feed.

154. At approximately the same time, advertisements from Credit Karma advertising random credit cards began appearing in Plaintiff Shah's Facebook feed.

155. Around the same time, other credit card providers advertising their own cards began appearing in Plaintiff Shah's Facebook feed.

156. Plaintiff Devin Rose has a Venture One credit card with Capital One.

157. Plaintiff Rose has been Defendant's customer since March 2024, when he applied for the Capital One Venture One credit card.

158. Plaintiff Rose was approved for the Capital One Venture One credit card and has used the card at least in California since being approved.

159. Plaintiff Rose has used Capital One's Website to facilitate his financial services with Defendant since March 2024 and inputted Personal and Financial Information into Defendant's Website at Defendant's direction and encouragement.

160. Plaintiff Rose used Capital One's Website to apply for a credit card.

161. Plaintiff Rose is a Facebook user, who joined Facebook at least ten years ago.

162. Shortly after Plaintiff Rose used Defendant's Website to apply for his Capital One Venture One credit card, Capital One credit card advertisements began appearing in his Facebook feed.

163. At approximately the same time, advertisements from other credit cards and for personal and business loans began appearing in Plaintiff Rose's Facebook feed.

164. Plaintiff Gary Ingraham does not have an active account with Capital One.

165. Plaintiff Ingraham applied for a Capital One credit card in or around May 2024.

166. Plaintiff Ingraham was not approved for a Capital One credit card.

167. Plaintiff Ingraham used Capital One's Website to apply for a credit card and inputted Personal and Financial Information into Defendant's Website at Defendant's direction and encouragement

168. Plaintiff Ingraham is a Facebook user.

169. Shortly after Plaintiff Ingraham used Defendant's Website to apply for a Capital One credit card, advertisements from Discover Cards began appearing in his Facebook feed.

170. At approximately the same time, advertisements from Chase Credit began appearing in Plaintiff Ingraham's Facebook feed.

171. Around the same time, advertisements from Chime began appearing in Plaintiff Ingraham's Facebook feed.

172. Plaintiff Deia Williams does not have an active account with Capital One.

173. Plaintiff Williams applied for a Capital One Venture card in 2023 and inputted Personal and Financial Information into Defendant's Website at Defendant's direction and encouragement.

174. Plaintiff Williams was not approved for a Capital One credit card.

175. Plaintiff Williams used Capital One's Website to apply for a credit card.

176. Plaintiff Williams is a Facebook user.

177. Shortly after Plaintiff Williams used Defendant's Website to apply for a Capital One credit card, she was constantly bombarded with credit card advertisements on Facebook.

178. Plaintiff Williams blocked Capital One on social media due to the bombardment of targeted advertising.

179. Plaintiffs accessed Defendant's Website at Defendant's direction and encouragement.

180. Plaintiffs relied on Defendant's Website to communicate Personal and Financial Information and did so with the understanding that Capital One would not share their Personal and Financial Information except as agreed in the Privacy Policies.

181. At no point did Customers like Plaintiffs sign any written authorization permitting Defendant to send their Personal and Financial Information to Third Parties (or fourth parties) uninvolved in providing them with financial services.

182. Plaintiffs reasonably expected that their communications with Capital One were confidential, solely between each Plaintiff and Capital One, and that, as such, those communications and any Personal and Financial Information submitted would not be transmitted to or intercepted by a third party (or used by a fourth party).

183. Plaintiffs provided their Personal and Financial Information to Defendant and trusted that the information would be safeguarded according to Capital One's promises and the law.

184. Plaintiffs never intended to sell their Personal and Financial Information, nor would they have permitted it to be made available for sale on the resale market.

185. Plaintiffs never intended to let Capital One benefit from their Personal and Financial Information.

186. Through the systematic data sharing process described in this complaint, Plaintiffs' interactions with Capital One's online financial platform were disclosed to third parties, including Facebook. Plaintiffs did not consent to those disclosures.

187. On information and belief, through its use of Third Party trackers on its Website, Defendant disclosed to Third Parties information Plaintiffs provided to Capital One as a financial institution and resulting from a transaction for Plaintiffs to obtain Defendant's credit card, including each Plaintiffs':

a. Employment information;

b. Bank account information (including, at a minimum, types of bank accounts);

c. Citizenship and dual citizenship status;

d. Credit card preapproval or eligibility;

e. Credit card approval or eligibility;

f. Plaintiffs' existing user, or Customer, status;

g. Browsing activities, including the pages and content Plaintiffs viewed;

h. That Plaintiffs were applying for a credit card (their status as a Customer); and

i. Information collected through an Internet "cookie" (or information collecting device from a web server).

188. By failing to receive the requisite consent, Capital One breached confidentiality and unlawfully disclosed Plaintiffs' Personal and Financial Information.

189. Plaintiffs would not have submitted their information to Capital One if they had known it would be shared with Third Parties and fourth parties.

190. As a result of Capital One's Disclosure of Plaintiffs' Personal and Financial Information via the Facebook Pixel and other tracking technologies to Third Parties (and fourth parties) without authorization, Plaintiffs suffered the following injuries:

a. Loss of privacy; unauthorized disclosure of their Personal and Financial Information; unauthorized access of their Personal and Financial Information by Third Parties;

b. Capital One benefited from the use of Plaintiffs' Personal and Financial Information without sharing that benefit with Plaintiffs;

c. Plaintiffs now receive targeted advertisements from fourth parties on social media, reflecting their Personal and Financial Information that was improperly disclosed and used;

d. Plaintiffs paid Capital One for financial services, and the services they paid for included reasonable privacy and data security protections for their Personal and Financial Information, but due to Defendant's Disclosure, Plaintiffs did not receive the privacy and security protections for which they paid;

e. The portion of Capital One's revenues and profits attributable to collecting Plaintiffs' Personal and Financial Information without authorization and sharing it with Third Parties (and fourth parties);

f. The portion of Capital One's savings in marketing costs attributable to collecting Plaintiffs' Personal and Financial Information without authorization and sharing it with Third Parties (and fourth parties);

g. The portion of Capital One's revenues and profits attributable to serving and monetizing advertisements directed to Plaintiffs as a result of collecting Plaintiffs' Personal and Financial Information without authorization and sharing it with Third Parties (and fourth parties);

h. Value to Plaintiffs of surrendering their choice to keep their Personal and Financial Information private and allowing Capital One to track their data;

i. Embarrassment, humiliation, frustration, and emotional distress;

j. Decreased value of Plaintiffs' Personal and Financial Information;

k. Lost benefit of the bargain;

l. Increased risk of future harm resulting from future use and disclosure of their Personal and Financial Information; and

m. Statutory damages.

**TOLLING, CONCEALMENT, AND ESTOPPEL**

191. The applicable statutes of limitation have been tolled as a result of Capital One's knowing and active concealment and denial of the facts alleged herein.

192. Capital One seamlessly incorporated trackers into its Website while providing Customers using those platforms with no indication that their Website usage was being tracked and transmitted to Third Parties. Capital One knew that its Website incorporated trackers, yet it failed to disclose to Plaintiffs and Class Members that their sensitive Personal and Financial Information would be intercepted, collected, used by, and disclosed to Third Parties.

193. Plaintiffs and Class Members could not with due diligence have discovered the full scope of Capital One's conduct, because there were no disclosures or other indication that they

were interacting with websites employing tracking technology to unauthorizedly disclose their Personal and Financial Information.

194. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. Capital One's illegal interception and disclosure of Plaintiffs' and the Class's Personal and Financial Information has continued unabated. What is more, Capital One was under a duty to disclose the nature and significance of its data collection practices but did not do so. Capital One is therefore estopped from relying on any statute of limitations defenses.

## CLASS ACTION ALLEGATIONS

195. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all other similarly situated persons pursuant to Fed. R. Civ. P. 23.

196. Plaintiffs seek to represent the following classes:

> **Nationwide Class**: All individuals in the United States whose Personal and Financial Information was disclosed by Defendant to Third Parties through Defendant's Website's tracking technology without authorization.
>
> **California Subclass**: All individuals in California whose Personal and Financial Information was disclosed by Defendant to Third Parties through Defendant's Website's tracking technology without authorization.

197. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

198. Plaintiffs reserve the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

199. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23(a)(1)-(4).

200. Numerosity: Class Members are so numerous and geographically dispersed that joinder of all members is impracticable. Upon information and belief, there likely millions of individuals throughout the United States whose Personal and Financial Information has been improperly used or disclosed by Defendant, and the Classes are identifiable within Defendant's records.

201. Ascertainability. Class Members are readily identifiable from information in Defendant's possession, custody, and control.

202. Commonality and Predominance: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether Defendant disclosed Class Members' Personal and Financial Information to Third Parties;

b. Whether Class Members consented to Defendant's disclosure of their Personal and Financial Information;

c. Whether Defendant owed duties to Plaintiffs and Class Members to protect their Personal and Financial Information;

d. Whether Defendant breached its duty to protect Plaintiffs' and Class Members' Personal and Financial Information;

e. Whether Defendant's disclosure of Plaintiffs' and Class Members' Personal and Financial Information to Third Parties violated federal, state and local laws, or industry standards;

f. Whether Defendant's failure to allow Customers a meaningful opportunity to opt out of sharing with Third Parties violated federal, state and local laws, or industry standards;

g. Whether Defendant's conduct resulted in or was the actual cause of the disclosure of Plaintiffs' and Class Members' and Personal and Financial Information;

h. Whether Defendant's conduct resulted in or was the proximate cause of the disclosure of Plaintiffs' and Class Members' Personal and Financial Information;

i. Whether Defendant has a contractual obligation to protect Plaintiffs' and Class Members' Personal and Financial Information and whether it complied with such contractual obligation;

j. Whether Defendant has a duty sounding in bailment to protect Plaintiffs' and Class Members' Personal and Financial Information and whether it complied with such obligation;

k. Whether Defendant has a duty of confidence and whether it complied with such obligation;

l. Whether Defendant's conduct amounted to violations of state consumer protection statutes;

m. Whether Defendant's conduct amounted to violations of state and federal wiretap statutes;

n. Whether Defendant's conduct amounted to violations of other California and Virginia state laws;

o. Whether Defendant should retain Plaintiffs' and Class Members' valuable Personal and Financial Information;

p. Whether, as a result of Defendant's conduct, Plaintiffs and Class Members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief.

203. Defendant has engaged in a common course of conduct toward Plaintiffs and the Class Members, in that the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully disclosed and accessed in the same way. As set forth above, the common issues arising from Defendant's conduct affecting Class Members predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

204. Typicality: Plaintiffs' claims are typical of those of other Class Members because all had their Personal and Financial Information compromised as a result of Defendant's use and incorporation of Facebook Pixel and other tracking technology.

205. Policies Generally Applicable to the Classes: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly, and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.

206. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages Plaintiffs have

suffered is typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intends to prosecute this action vigorously.

207. Superiority and Manageability: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

208. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged. If the class action device were not used, Defendant would necessarily gain an unconscionable advantage because it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources. Moreover, the costs of individual suits could unreasonably consume the amounts that would be recovered, whereas proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged. Finally, individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

209. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

210. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

211. Unless a Class-wide injunction is issued, Defendant may continue in its unlawful use and disclosure and failure to properly secure the Personal and Financial Information of Plaintiffs and the Class Members, Defendant may continue to refuse to provide proper notification to and obtain proper consent from Class Member, and Defendant may continue to act unlawfully as set forth in this Complaint.

212. Moreover, Defendant has acted or refused to act on grounds generally applicable to the Class, and, accordingly, final injunctive or corresponding declaratory relief regarding the whole of the Classes is appropriate.

213. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Personal and Financial Information;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Personal and Financial Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to the disclosure of customer information;

d. Whether Defendant was negligent and/or negligent *per se*;

e. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that contract;

f. Whether Defendant breached the contract;

g. In the alternate, whether Defendant was unjustly enriched;

h. Whether a bailment existed between Defendant on the one hand, and Plaintiffs and Class Members on the other;

i. Whether Defendant breached its bailment duty;

j. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Personal and Financial Information had been used and disclosed to Third Parties and used for Third Party and fourth party benefit;

k. Whether Defendant adequately provided opt-out measures;

l. Whether Defendant abided by Plaintiffs' and Class Members' opt-out requests;

m. Whether Defendant failed to implement and maintain reasonable security procedures and practices;

n. Whether Defendant invaded Plaintiffs and the Class Members' privacy;

o. Whether Defendant breached its implied duty of confidentiality; and,

p. Whether Plaintiffs and the Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

**COUNT I**
**NEGLIGENCE**
**(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

214. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

215. Plaintiffs and Class Members submitted sensitive nonpublic personal information, including Personal and Financial Information, when accessing Capital One's Website.

216. Defendant owed to Plaintiffs and Class Members a duty to exercise reasonable care in handling and using Plaintiffs' and Class Members' Personal and Financial Information in its care and custody, including implementing industry-standard privacy procedures sufficient to reasonably protect the information from the disclosure and unauthorized transmittal and use of Personal and Financial Information that occurred.

217. Defendant's duties to keep the nonpublic personal information, including Personal and Financial Information, confidential also arose under the GLBA, which imposes "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801(a).

218. Defendant's duties to keep the nonpublic personal information, including Personal and Financial Information, confidential also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including the unfair practice of failing to keep the nonpublic personal information confidential.

219. Defendant acted with wanton and reckless disregard for the privacy and confidentiality of Plaintiffs' and Class Members' Personal and Financial Information by disclosing

and providing access to this information to the Third Parties for the financial benefit of the Third Parties (and fourth parties) and Defendant.

220. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's disclosure of their Personal and Financial Information to benefit Third Parties (and fourth parties) and Defendant. Defendant actively sought and obtained Plaintiffs' and Class Members' Personal and Financial Information. And Defendant knew or should have known that by integrating tracking technology on its Website that Plaintiffs' and Class Members' nonpublic personal information, including Personal and Financial Information, would be disclosed to the Third Parties (and used by the fourth parties).

221. Personal and Financial Information is highly valuable, and Defendant knew, or should have known, the harm that would be inflicted on Plaintiffs and Class Members by disclosing their Personal and Financial Information to the Third Parties. This disclosure was of benefit to the Third Parties (and fourth parties) and Defendant by way of data harvesting, advertising, and increased sales.

222. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers in the handling and securing of Personal and Financial Information of Plaintiffs and Class Members. This failure actually and proximately caused Plaintiffs' and Class Members' injuries.

223. As a direct, proximate, and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or imminently will suffer injury and damages, including monetary damages, inappropriate advertisements and use of their Personal

and Financial Information for advertising purposes, and increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

224. Defendant's breach of its common-law duties to exercise reasonable care and negligence, directly and proximately caused Plaintiffs' and Class Members' actual, tangible, injury-in-fact and damages, including, without limitation: the unauthorized access of their Personal and Financial Information by Third Parties (and fourth parties); improper disclosure of their Personal and Financial Information; receipt of targeted advertisements reflecting private medical information; lost benefit of their bargain; lost value of their Personal and Financial Information and diminution in value; embarrassment, humiliation, frustration, and emotional distress; lost time and money incurred to mitigate and remediate the effects of use of their information, as to targeted advertisements that resulted from and were caused by Defendant's negligence; value to Plaintiffs and the Class Members of surrendering their choices to keep their Personal and Financial Information private and allowing Defendant to track their data; increased risk of future harm resulting from future use and disclosure of Plaintiffs' and the Class Members' Personal and Financial Information; and other injuries and damages as set forth herein. These injuries are ongoing, imminent, immediate, and continuing.

225. Defendant's negligence directly and proximately caused the unauthorized access and Disclosure of Plaintiffs' and Class Members' Personal and Financial Information, and as a result, Plaintiffs and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiffs and Class Members seek actual and compensatory damages, and all other relief they may be entitled to as a proximate result of Defendant's negligence.

226. Plaintiffs and Class Members seek to recover the value of the unauthorized access to their Personal and Financial Information resulting from Defendant's wrongful conduct. This

measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's personal information is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a Plaintiffs may generally recover the reasonable use value of the IP—i.e., a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non-practicing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiffs and Class Members have a protectible property interest in their Personal and Financial Information; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, i.e., evidence regarding the value of similar transactions

227. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

**COUNT II**
**NEGLIGENCE *PER SE***
**(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

228. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

229. Plaintiffs being this negligence *per se* count in the alternative to their common law negligence claim.

230. Pursuant to the laws set forth herein, including the FTC Act, the GLBA, and state law, Defendant was required by law and industry standards to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiffs' and Class Members' Personal and Financial Information.

231. Plaintiffs and Class Members are within the class of persons that these statutes and rules were designed to protect.

232. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' Personal and Financial Information.

233. Defendant owed a duty to timely and adequately inform Plaintiffs and Class Members, in the event of their Personal and Financial Information being improperly disclosed to unauthorized Third Parties.

234. It was not only reasonably foreseeable, but it was intended, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Personal and Financial Information in compliance with applicable laws would result in unauthorized Third Parties gaining access to Plaintiffs' and Class Members' Personal and Financial Information, and resulting in Defendant's liability under principles of negligence *per se*.

235. Defendant violated its duty under Section 5 of the FTC Act, the GLBA, and/or state law by failing to use reasonable measures to protect Plaintiffs' and Class Members' Personal and Financial Information and not complying with applicable industry standards as described in detail herein.

236. Plaintiffs' and Class Member's Personal and Financial Information constitutes personal property that was taken and misused as a proximate result of Defendant's negligence, resulting in harm, injury and damages to Plaintiffs and Class Members.

237. As a proximate result of Defendant's negligence *per se* and breach of duties as set forth above, Plaintiffs and Class Members were caused to, *inter alia*, have their data shared with Third Parties without their authorization or consent, receive unwanted advertisements that reveal seeking treatment for specific medical conditions, fear, anxiety and worry about the status of their Personal and Financial Information, diminution in the value of their personal data for which there is a tangible value, and/or a loss of control over their Personal and Financial Information, all of which can constitute actionable actual damages.

238. Defendant's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiffs' and Class Members' Personal and Financial Information, and as a result, Plaintiffs and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiffs and Class Members seek actual, and compensatory damages, and all other relief they may be entitled to as a proximate result of Defendant's negligence *per se*.

239. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

**COUNT III**
**INVASION OF PRIVACY**
**Cal. Const. Art. 1 § 1**
**(On Behalf of Plaintiffs and the California Subclass)**

240. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

241. California established the right to privacy in Article I, Section I of the California Constitution.

242. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Website.

243. Plaintiffs and Class Members communicated sensitive Personal and Financial Information that they intended for only Defendant to receive and that they understood Defendant would keep private.

244. Defendant's disclosure of the substance and nature of those communications to Third Parties without the knowledge and consent of Plaintiffs and Class Members is an intentional intrusion on Plaintiffs' and Class Members' solitude or seclusion in their private affairs and concerns.

245. Plaintiffs and Class Members had a reasonable expectation of privacy given their relationship with Defendant as a financial institution. Moreover, Plaintiffs and Class Members have a general expectation that their communications regarding Personal and Financial Information with their financial institution will be kept confidential. Defendant's disclosure of Personal and Financial Information is highly offensive to the reasonable person.

246. As a result of Defendant's actions, Plaintiffs and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights under the California Constitution.

247. Plaintiffs and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

248. Plaintiffs and Class Members seek appropriate relief for that injury, including but not limited to, damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests as a result of its intrusions upon Plaintiffs' and Class Members' privacy.

249. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

250. Plaintiffs also seek such other relief as the Court may deem just and proper.

**COUNT IV**
**VIOLATION OF THE COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT, CAL. PENAL CODE § 502**
**(On Behalf of Plaintiffs and the California Subclass)**

251. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

252. The California Legislature enacted the Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502 to "expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems," and finding and declaring "that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data." Cal. Penal Code § 502(a).

253. In enacting the CDAFA, the Legislature further found and declared "that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data." Cal. Penal Code § 502(a).

254. Plaintiffs' and the Class Members' devices on which they accessed Defendant's Online Platforms and Websites, including their computers, smart phones, and tablets, constitute computers or "computer systems" within the meaning of CDAFA. Cal. Penal Code § 502(b)(5).

255. By conduct complained of in the preceding paragraphs, Defendant violated Section 502(c)(1)(B) of CDAFA by knowingly accessing without permission Plaintiffs' and Class Members' devices in order to wrongfully obtain and use their personal data, including their Personal and Financial Information, in violation of Plaintiffs' and Class Members' reasonable expectations of privacy in their devices and data.

256. Defendant violated Cal. Penal Code § 502(c)(2) by knowingly and without permission accessing, taking, copying, and using Plaintiffs' and the Class Members' Personal and Financial Information.

257. Defendant used Plaintiffs' and Class Members' data as part of a scheme to defraud them and wrongfully obtain their data and other economic benefits. Specifically, Defendant intentionally concealed from Plaintiffs and Class Members that Defendant had secretly installed tracking pixels on its Online Platforms that surreptitiously shared Personal and Financial Information with third party advertising companies like Facebook. Had Plaintiffs and Class Members been aware of this practice, they would not have used Defendant's Website and Online Platforms.

258. The computers and mobile devices that Plaintiffs and Class Members used when accessing Defendant's Website all have and operate "computer services" within the meaning of CDAFA. Defendant violated §§ 502(c)( of CDAFA by knowingly and without permission accessing and using those devices and computer services, and/or causing them to be accessed and used, *inter alia*, in connection with the Third Parties' (and fourth parties') wrongful use of such data.

259. Under § 502(b)(12) of the CDAFA a "Computer contaminant" is defined as "any set of computer instructions that are designed to . . . record, or transmit information within a

computer, computer system, or computer network without the intent or permission of the owner of the information."

260. Defendant violated § 502(c)(8) by knowingly and without permission introducing a computer contaminant via trackers embedded into the Online Platforms which intercepted Plaintiffs' and the Class Members' private and sensitive financial information.

261. Defendant's violation of the CDAFA caused Plaintiffs and Class Members, at minimum, the following damages:

a. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private;

b. Defendant eroded the essential confidential nature of their relationship;

c. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without sharing the benefit of such value;

d. Plaintiffs and Class Members did not get the full value of the financial services for which they paid, which included Defendant's duty to maintain confidentiality; and

e. Defendant's actions diminished the value of Plaintiffs' and Class Members' Private Information.

262. Plaintiffs and the Class Members seek compensatory damages in accordance with Cal. Penal Code § 502(e)(1), in an amount to be proved at trial, and injunctive or other equitable relief; as well as punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) as Defendant's violations were willful and, upon information and belief, Defendant is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294; and reasonable attorney's fees under § 502(e)(2).

263. Plaintiffs and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

**COUNT V**
**VIOLATION OF CALIFORNIA'S CONSUMER PROTECTION LAW ("UCL"), CAL. BUS. & PROF. CODE §§ 17200, *et seq.***
**(On Behalf of Plaintiffs and the California subclass)**

264. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

265. Plaintiffs and Defendant are each a "person" under Cal. Bus. & Prof. Code § 17201.

266. The California Business and Professions Code §§ 17201, *et seq*. prohibits acts of unfair competition, which includes unlawful business practices.

267. Defendant's business acts and practices are "unlawful" under the Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200 *et. seq.* (the "UCL") because, as alleged above, Defendant violated California common law, and other statutes and causes of action alleged herein.

268. Defendant engaged in unlawful acts and practices by imbedding the Pixel on its Websites, which tracks, records, and transmits Plaintiffs' and Class Members' Personal and Financial Information they disclose to Defendant in confidence its Website to Third Parties without Plaintiffs' and Class Members' knowledge and/or consent, in violation of the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq*.; the Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502; and by representing that their services have characteristics, uses, or benefits that they do not have in violation of Civil Code § 1770.

269. When using Defendant's Website and services, Plaintiffs and Class Members relied on Defendant's status as a trusted financial institution.

270. Inconsistent with its role as a financial service provider, Defendant disclosed Plaintiffs' and Class Members' Personal and Financial Information to Third Parties without their consent and for marketing purposes. Thus, Defendant represented that its services have

characteristics, uses, or benefits that they do not have and represented that its services are of a particular standard, quality, or grade when they were not, in violation of Cal. Civil Code § 1770.

271. Plaintiffs and Class Members were reasonable to assume, and did assume, that Defendant would take appropriate measures to keep their Personal and Financial Information secure and not share it with Third Parties, or allow Third Parties (and fourth parties) to use it,without their express consent. Defendant also had a duty to disclose that it was sharing their Customers' Personal and Financial Information with Third Parties. However, Defendant did not disclose at any time that it was sharing this Personal and Financial Information with Third Parties via tracking technologies or that Third Parties (and fourth parties) were using their Personal and Financial Information.

272. Had Plaintiffs and Class Members known that Defendant would intercept, collect, and transmit their Personal and Financial Information to Third Parties, Plaintiffs and the Class Members would not have used Defendant's services.

273. Plaintiffs and Class Members have a property interest in their Personal and Financial Information. By surreptitiously collecting and otherwise misusing Plaintiffs' and Class Members' Personal and Financial Information, Defendant has taken property from Plaintiffs and Class Members without providing just (or indeed any) compensation.

274. By deceptively collecting, using, and sharing Plaintiffs' and Class Members' Personal and Financial Information with Third Parties for Third Party (and fourth parties) use, Defendant have taken money or property from Plaintiffs and Class Members. Accordingly, Plaintiffs seek restitution on behalf of themselves and the Class.

275. Defendant's business acts and practices also meet the unfairness prong of California's Unfair Competition Law ("UCL") according to all three theories of unfairness.

276. First, Defendant's business acts and practices are "unfair" under the UCL pursuant to the three-part test articulated in *Camacho v. Automobile Club of Southern California* (2006) 142 Cal. App. 4th 1394, 1403: (a) Plaintiffs and Class Members suffered substantial injury due to Defendant's Disclosure of their Personal and Financial Information; (b) Defendant's disclosure of Plaintiffs' and Class Members' Personal and Financial Information provides no benefit to Customers, let alone any countervailing benefit that could justify Defendant's Disclosure of Personal and Financial Information without consent for marketing purposes or other pecuniary gain; and (c) Plaintiffs and Class Members could not have readily avoided this injury because they had no way of knowing that Defendant was implementing tracking technology.

277. Second, Defendant's business acts and practices are "unfair" under the UCL because they are "immoral, unethical, oppressive, unscrupulous, or substantially injurious" to Plaintiffs and Class Members, and "the utility of [Defendant's] conduct," if any, does not "outweigh the gravity of the harm" to Plaintiffs and Class Members. *Drum v. San Fernando Valley Bar Ass'n,* (2010) 182 Cal. App. 4th 247, 257. Defendant secretly collected, disclosed, and otherwise misused Plaintiffs' and Class Members' Personal and Financial Information by bartering it to Third Parties in return for marketing and profit. This surreptitious, willful, and undisclosed conduct is immoral, unethical, oppressive, unscrupulous, and substantially injurious. Moreover, no benefit inheres in this conduct, the gravity of which is significant.

278. Third, Defendant's business acts and practices are "unfair" under the UCL because they run afoul of "specific constitutional, statutory, or regulatory provisions." *Drum*, 182 Cal. App. 4th at 256 (internal quotation marks and citations omitted). California has a strong public policy of protecting consumers' privacy interests, including consumers' personal data, as codified in California's Constitution in Article I, section 1; the California Invasion of Privacy Act, Cal. Penal

Code §§ 630, *et seq*.; and the Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502, among other statutes.

279. Defendant violated this public policy by, among other things, surreptitiously collecting, disclosing, and otherwise exploiting Plaintiffs' and Class Members' Personal and Financial Information by sharing that information with Third Parties via tracking technologies without Plaintiffs' and/or Class Members' consent.

280. Had Plaintiffs and Class Members known Defendant would intercept, collect, and transmit their Personal and Financial Information to Facebook and other Third Parties, Plaintiffs and Class Members would not have used Defendant's services.

281. Plaintiffs and Class Members were reasonable to assume, and did assume, that Defendant would take appropriate measures to keep their Personal and Financial Information secure and not share it with Third Parties without their express consent. Defendant was in sole possession of and had a duty to disclose the material information that Plaintiffs' and Class Members' Personal and Financial Information would be shared with Third Parties via trackers. Defendant did not disclose at any time that they were sharing this Personal and Financial Information with Third Parties via trackers.

282. Plaintiffs and Class Members have a property interest in their Personal and Financial Information. By surreptitiously collecting and otherwise misusing Plaintiffs' and Class Members' Personal and Financial Information, Defendant has taken property from Plaintiffs and Class Members without providing just (or indeed any) compensation.

283. Plaintiffs and Class Members have lost money and property due to Defendant's conduct in violation of the UCL. Personal and Financial Information such as that which Defendant collected and transmitted to Third Parties has objective monetary value. Companies are willing to

pay for Personal and Financial Information, like the information Defendant unlawfully collected and transmitted to Third Parties. For example, Pfizer annually pays approximately $12 million to purchase similarly sensitive information on health data, from various sources.[108]

284. By deceptively collecting, using, and sharing Plaintiffs' and Class Members' Personal and Financial Information with Third Parties, and by allowing Third Parties (and fourth parties) to use their Personal and Financial Information, Defendant has taken money and/or property from Plaintiffs and Class Members. Accordingly, Plaintiffs seek restitution on behalf of themselves and the Class.

285. As a direct and proximate result of Defendant's unfair and unlawful methods and practices of competition, Plaintiffs and Class Members suffered actual damages, including, but not limited to, the loss of the value of their Personal and Financial Information.

286. As a direct and proximate result of its unfair and unlawful business practices, Defendant has each been unjustly enriched and should be required to make restitution to Plaintiffs and Class Members pursuant to §§ 17203 and 17204 of the California Business & Professions Code, disgorgement of all profits accruing to Defendant because of its unlawful and unfair business practices, declaratory relief, attorney fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5), and injunctive or other equitable relief.

**COUNT VI**
**VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT,**
**Cal. Civ. Code § 1798.100, *et seq.***
**(On Behalf of Plaintiffs and the California subclass)**

287. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

[108] SciAm, *How Data Brokers Make Money Off Your Medical Records*, https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/ (last visited Aug. 8, 2024).

288. The CCPA grants consumers rights, including the right to know what personal information is being collected about them and whether that information is sold or disclosed and to whom, the right to prohibit the sale of their personal information, the right to request deletion of their personal information, and the right to nondiscrimination in service and price when they exercise privacy rights. Ca. Civ. Code § 1798.100 *et seq*.

289. CCPA dictates specifically that "[a] third party shall not sell or share personal information about a consumer that has been sold to, or shared with, the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out." Cal. Civ. Code § 1798.115 (emphasis added).

290. Defendant collected Plaintiffs' and Class Members Personal and Financial Information, including their personal information, with the purpose of providing financial services in the course of and as part of its business in California.

291. Disclosing Customers,' like Plaintiffs' and Class Members,' Personal and Financial Information to Third Parties was not reasonably necessary or proportionate to perform the reasonably expected financial services that they applied for or received.

292. By collecting, using, and selling Plaintiffs' and Class Members' personal information and location data to Third Parties for Third Party (and fourth party) use, all without providing consumers with notice, Defendant violated CCPA.

293. By failing to inform Customers like Plaintiffs and Class Members of the personal information collected about them and the Third Parties with whom that personal information was shared, and the Third Parties' (and fourth parties') use of that personal information, Defendant violated CCPA.

294. By failing to provide Customers like Plaintiffs and Class Members with sufficient opt out opportunities, Defendant violated CCPA.

295. By further failing to abide by Plaintiffs' and Class Members' opt out requests, Defendant violated CCPA.

296. By failing to abide by Customers' requests to delete collected personal information, Defendant violated CCPA.

297. Pursuant to Ca. Civ. Code § 1798.150(b), Plaintiffs will send Defendant notice of their CCPA claims shortly after the date of this filing. If Defendant does not correct its business practices, Plaintiffs will amend (or seek leave to amend) the complaint to add claims for monetary relief, including statutory and actual damages under the CCPA. To date, Defendant has failed to cure the CCPA violation.

298. As a result of Defendant's reckless violations, Plaintiffs are entitled to actual damages, statutory damages, and attorneys' fees and costs. *Id.* at § 1798.150.

**COUNT VII**
**VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT,**
**CAL. CIV. CODE §§ 1798.80, *et seq.***
**(On Behalf of Plaintiffs and the California subclass)**

299. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

300. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Civil Code section 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

301. Defendant is a business that owns, maintains, and licenses personal information, within the meaning of 1798.81.5, about Plaintiffs and Class Members.

302. By failing to implement and maintain reasonable security procedures and practices with respect to Plaintiffs' and Class Members' personal information, Defendant violated Cal. Civ. Code § 1798.80 *et seq*.

303. Because Defendant reasonably knew that Plaintiffs' and Class Members' information was acquired by persons unauthorized by Plaintiffs and Class Members, Defendant has an obligation to disclose that in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

304. By failing to disclose to Plaintiffs and Class Members its Disclosure of their information to Third Parties, Defendant violated Cal. Civ. Code § 1798.82.

305. As a direct and proximate result of Defendant's violations of the Cal. Civ. Code §1798.80 *et seq.*, Plaintiffs and Class Members suffered damages, as described above.

**COUNT VIII**
**BREACH OF EXPRESS AND IMPLIED CONTRACT**
**(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

306. Plaintiffs re-allege and incorporate the preceding paragraphs as if fully set forth herein.

307. Plaintiffs and Class Members also entered into an express and implied contract with Capital One when they obtained financial services from Capital One, or otherwise provided nonpublic personal information, including Personal and Financial Information, to Capital One.

308. As part of these transactions, Capital One explicitly and implicitly agreed to safeguard and protect Plaintiffs' and Class Members' Personal and Financial Information.

309. Plaintiffs and Class Members entered into express and implied contracts with the reasonable expectation (based on Capital One's own express and implied promises) that Capital One would keep their nonpublic personal information, including Personal and Financial Information, confidential. Plaintiffs and Class Members believed that Capital One would use part of the monies paid to Capital One under the express and implied contracts to keep their nonpublic personal information, including Personal and Financial Information, confidential.

310. Plaintiffs and Class Members would not have provided and entrusted their nonpublic personal information, including Personal and Financial Information, or would have paid less for Capital One's services in the absence of the express and implied contract or implied terms between them and Capital One. The safeguarding of the nonpublic personal information, including Personal and Financial Information, of Plaintiffs and class members was critical to realize the intent of the parties.

311. As extensively detailed above, Capital One breached its express and implied contracts with Plaintiffs and class members to protect their nonpublic personal information, including Personal and Financial Information, when it disclosed that information to Third Parties.

312. As a direct and proximate result of Capital One's breach of express and implied contract, Plaintiffs and Class Members sustained actual losses and damages as described in detail above.

**COUNT IX**
**UNJUST ENRICHMENT (AS ALTERNATIVE TO CONTRACT CLAIMS)**
**(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

313. Plaintiffs re-allege and incorporate the preceding paragraphs as if fully set forth herein.

314. Plaintiffs and Class Members have an interest, both equitable and legal and financial, in their Personal and Financial Information, that was conferred upon, collected by, and maintained by Defendant and that was ultimately disclosed without their consent.

315. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of valuable, sensitive, personal, and financial information—Personal and Financial Information—that Defendant collected from Plaintiffs and Class Members under the guise of keeping this information private. Defendant collected, used, and disclosed this information for its own gain, for marketing purposes, and for sale or trade with Third Parties. Defendant did not share this benefit with Plaintiffs and Class Members.

316. Plaintiffs and Class Members would not have used Defendant's services, or would have paid less for those services, if they had known that Defendant would collect, use, and disclose their Personal and Financial Information to Third Parties or allow Third Parties (and fourth parties) to use their Personal and Financial Information.

317. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members.

318. The benefits that Defendant derived from Plaintiffs and Class Members rightly belong to Plaintiffs and Class Members themselves. Under unjust enrichment principles, it would be inequitable for Defendant to retain the profit and/or other benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

319. Defendant continues to benefit and profit from its retention and use of Plaintiffs' and Class Members' Personal and Financial Information, while its value to Plaintiffs and Class Members has been diminished.

320. Plaintiffs pleads this claim separately as well as in the alternative to claims for damages under Fed. R. Civ. P. 8(a)(3), because if the Court dismisses Plaintiffs' claims for damages or enters judgment on them in favor of the Defendant, Plaintiffs' will have no adequate legal remedy. Plaintiffs make the following allegations in this paragraph only hypothetically and as an alternative to any contrary allegations in her other causes of action, in the event that such causes of action do not succeed. Plaintiffs and the Class Members may be unable to obtain monetary, declaratory and/or injunctive relief directly under other causes of action, and, if so, will lack an adequate remedy at law.

321. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds it received as a result of the conduct and the unauthorized Disclosure alleged herein

**COUNT X**
**BAILMENT**
**(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

322. Plaintiffs re-allege and incorporate the preceding paragraphs as if fully set forth herein.

323. Plaintiffs, Class Members, and Defendant contemplated a mutual benefit bailment when Plaintiffs and Class Members transmitted their Personal and Financial Information to Defendant solely for financial services and the payment thereof.

324. Plaintiffs' and Class Members' Personal and Financial Information was transmitted to Defendant in trust for a specific and sole purpose of receiving Capital One's financial services, with an implied contract that the trust was to be faithfully executed, and the Personal and Financial Information was to be accounted for when the special purpose was accomplished.

325. Defendant was duty bound under the law to exercise ordinary care and diligence in safeguarding Plaintiffs' and Class Members' Personal and Financial Information.

326. Plaintiffs' and Class Members' Personal and Financial Information was used for a different purpose than Plaintiffs and Class Members intended, for a longer time period and/or in a different manner or place than the parties intended.

327. Defendant's breach of the bailment was a legal cause of injury-in-fact and damage to Plaintiffs and Class Members, including but not limited to, the unauthorized access of their Personal and Financial Information by Third Parties, improper use of their Personal and Financial Information by Third Parties, improper use of their Personal and Financial Information by fourth parties, improper disclosure of their Personal and Financial Information, lost benefit of their bargain, lost value of their Personal and Financial Information, and lost time and money incurred to mitigate and remediate the effects of use of their information that resulted from and were caused by Defendant's tortious conduct. These injuries are ongoing, imminent, immediate, and continuing.

328. As a direct and proximate result of Defendant's breach of the bailment, Plaintiffs and Class Members are entitled to and do demand actual, compensatory, and punitive damages, as well as injunctive relief, and all other relief allowed by law.

**COUNT XI**
**DECLARATORY JUDGMENT**
**(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

329. Plaintiffs re-allege and incorporate the preceding paragraphs as if fully set forth herein.

330. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, the Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant

further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this complaint.

331. An actual controversy has arisen regarding Capital One's present and prospective common law and other duties to keep its Customers' Personal and Financial Information confidential and whether Defendant is currently keeping that information confidential. Plaintiffs like Shah remain Capital One Customers who need to use the Capital One's Website to manage accounts and the financial services provided them by Capital One. Plaintiffs Shah, Rose, and similar Class Members thus remain at imminent risk that additional disclosure of their Personal and Financial Information will occur in the future.

332. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant continues to owe a legal duty to secure Customers' Personal and Financial Information, under the common law, Section 5 of the FTC Act, the GLBA, and various state statutes;

b. Defendant continues to breach this legal duty by disclosing its Customers' Personal and Financial Information, to unaffiliated Third Parties.

333. The Court also should issue corresponding prospective injunctive relief requiring Defendant to keep its nonpublic personal information, including Personal and Financial Information, confidential consistent with law and industry standards.

334. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy. The risk of additional disclosure is real, immediate, and substantial, as trackers remain operative on Defendant's website to this day. If additional disclosure occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of

the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

335. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if Capital One continues to disclose its Customers' Personal and Financial Information, Plaintiffs and Class Members will likely be subjected to the harms described herein. On the other hand, the cost to Defendant of complying with an injunction by keeping its Customers' Personal and Financial Information, confidential is relatively minimal (for example, removing trackers from its website), and Defendant has a pre-existing legal obligation to do so.

336. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing Capital One's additional unlawful disclosures of Customers' Personal and Financial Information, thus eliminating the additional injuries that would result to Plaintiffs and the hundreds of thousands of Customers whose information has been and will continue to be disclosed.

**COUNT XII**
**BREACH OF CONFIDENCE**
**(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

337. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

338. At all times during Plaintiffs' and Class Members' interactions with Capital One, Capital One was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' Personal and Financial Information.

339. As alleged herein and above, Capital One's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' Personal and Financial Information, would be collected, stored, and protected in confidence, and would not

be disclosed to Third Parties, or used by Third Parties (and fourth parties) without notice and consent.

340. Plaintiffs and Class Members provided Capital One with their Personal and Financial Information, with the explicit and implicit understandings that Capital One would protect and not permit that information to be disseminated to and used by unaffiliated Third Parties (and fourth parties) without notice, consent, and sufficient opportunity to opt out.

341. Capital One voluntarily received in confidence Plaintiffs' and Class Members' Personal and Financial Information, with the understanding and affirmative representation to Customers that the information would not be disclosed or disseminated to unaffiliated Third Parties for Third Parties' (and fourth parties') marketing purposes.

342. Capital One disclosed Plaintiffs' and Class Members' Personal and Financial Information, without notice, without express permission, and without opportunity to opt out.

343. But for Capital One's Disclosure of Plaintiffs' and Class Members' Personal and Financial Information, in violation of the parties' understanding of confidence, their Personal and Financial Information would not have been disclosed to Third Parties, or used for Third Party (and fourth party) marketing and profit, without their consent.

344. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Capital One's nonconsensual disclosure of Plaintiffs' and Class Members' Personal and Financial Information. Capital One knew it was disclosing Plaintiffs' and Class Members' Personal and Financial Information to Third Parties, for Third Party (and fourth party) use, without their consent.

345. As a direct and proximate result of Capital One's breaches of confidence, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial.

346. Plaintiffs seek all monetary and non-monetary relief allowed by law.

**COUNT XIII**
**VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT,**
**CAL. PENAL CODE §§ 630, *et seq.***
**(On Behalf of Plaintiffs and the California Subclass)**

347. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

348. The California Legislature enacted the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq*. declaring that:

> …advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.
>
> The Legislature by this chapter intends to protect the right of privacy of the people of this state.

Cal. Penal Code §§ 630.

349. Cal. Penal Code § 631(a) prohibits persons from "aid[ing], agree[ing] with, employ[ing], or conspir[ing] with" a third party to "read[], or attempt[] 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 who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained" "by means of any machine, instrument, or contrivance, or in any other manner…" Cal. Penal Code § 631(a).

350. Cal. Penal Code § 632(a) prohibits persons from intentionally recording confidential communications without consent of all parties to the communication.

351. All alleged communications between individual Plaintiffs or Class Members and Defendant qualify as protected communications under CIPA because each communication is made using personal computing devices (e.g., computers, smartphones, tablets) that send and receive communications in whole or in part through the use of facilities used for the transmission of communications aided by wire, cable, or other like connections.

352. As alleged in the preceding paragraphs, by use of the tracking technology, Defendant used a recording device to record the confidential communications including Personal and Financial Information without the consent of Plaintiffs or Class Members and then transmitted such information to Third Parties for Third Party (and fourth party) use.

353. At all relevant times, Defendant's aiding of Third Parties to learn the contents of communications and Defendant's recording of confidential communications was without Plaintiffs' and the Class Members' authorization and consent.

354. Plaintiffs and Class Members had a reasonable expectation of privacy regarding the confidentiality of their communications with Defendant. Defendant had duties under statutory and common law to safeguard its Customers' Personal and Financial Information, and not disclose it without authorization. Defendant never received any authorization and disclosed Plaintiffs' and the Class's Personal and Financial Information regardless.

355. Defendant engaged in and continued to engage in interception by aiding others (including Facebook) to secretly record the contents of Plaintiffs' and Class Members' wire communications.

356. The intercepting devices used in this case include, but are not limited to:

a. Those to which Plaintiffs' and Class Members' communications were disclosed;

b. Plaintiffs' and Class Members' personal computing devices;

c. Plaintiffs' and Class Members' web browsers;

d. Plaintiffs' and Class Members' browser-managed files;

e. Trackers like the Meta Pixel;

f. Internet cookies;

g. Other pixels, trackers, and/or tracking technology installed on Defendant's Website and/or server;

h. Defendant's computer servers;

i. Third Party source code utilized by Defendant; and

j. Third Party computer servers (including Facebook).

357. Defendant aided in the interception of contents in that the data from the communications between Plaintiffs and/or Class Members and Defendant that were redirected to and recorded by the Third Parties include information which identifies the parties to each communication, their existence, and their contents.

358. Plaintiffs and Class Members reasonably expected that their Personal and Financial Information was not being intercepted, recorded, and disclosed to Third Parties or used by Third Parties (and fourth parties) for marketing and profit.

359. No legitimate purpose was served by Defendant's willful and intentional disclosure of Plaintiffs' and Class Members' Personal and Financial Information to Third Parties. Neither Plaintiffs nor Class Members consented to the disclosure of their Personal and Financial Information by Defendant to Third Parties or the use of the Personal and Financial Information by Third Parties (and fourth parties).

360. The trackers that Defendant utilized are designed such that they transmitted each of a website user's actions to Third Parties alongside and contemporaneously with the user initiating the communication. Thus, Plaintiffs and Class Members' communications were intercepted in transit to the intended recipient (Defendant) before they reached Defendant's servers.

361. Defendant willingly facilitated the Third Parties' interception and collection of Plaintiffs' and Class Members' Personal and Financial Information, and the Third Parties' (and fourth parties') use of their Personal and Financial Information, by embedding trackers on its Website. Moreover, Defendant had full control over these trackers, including which webpages contained the pixels, what information was tracked and shared, and how events were categorized prior to transmission.

362. Defendant gave substantial assistance to Third Parties in violating the privacy rights of Capital One's Customers, even though Defendant's conduct constituted a breach of the confidentiality duties that it owed, including the duty financial institutions owe to their customers and customers' property. Defendant knew that the installation of trackers on its website would result in the unauthorized disclosure of its Customers' communications to Third Parties, and Third Party (and fourth party) use of those communications, yet nevertheless did so anyway.

363. Plaintiffs' and Class Members' electronic communications were intercepted during transmission, without their consent, for the unlawful and/or wrongful purpose of monetizing their Personal and Financial Information, including using their Personal and Financial Information to develop marketing and advertising strategies.

364. The Personal and Financial Information that Defendant assisted Third Parties with reading, learning, and exploiting, included Plaintiffs' and Class Members' Personal and Financial Information customers input into and accessed on Capital One's Website. Capital One disclosed

details about Customers, like Plaintiffs and Class Personal and Financial Information and their interactions with Capital One's website as users applied for credit cards, including the fact that a user was on a certain page, that users clicked buttons and what URLs or webpages they led to, information entered on preapproval application pages including employment, bank accounts, and Customers' eligibility, pre-approval, or approval for a credit card.

365. Plaintiffs and the Class Members seek statutory damages under Cal. Penal Code § 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 Classes in an amount to be proven at trial, as well as injunctive or other equitable relief.

366. In addition to statutory damages, Defendant's violations caused Plaintiffs and Class Members the following damages.

a. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private.

b. Defendant eroded the essential confidential nature of the banker-customer, and specifically the creditor-debtor, relationship.

c. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without sharing the benefit of such value;

d. Plaintiffs and Class Members did not get the full value of the financial services for which they paid, which included Defendant's duty to maintain confidentiality; and

e. Defendant's actions diminished the value of Plaintiffs' and Class Members' Personal and Financial Information.

367. Plaintiffs and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

**COUNT XIV**
**VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")**
**18 U.S.C. §§ 2511(1), *et seq.***
**(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

368. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

369. The ECPA protects both sending and receipt of communications. 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.

370. The transmissions of Plaintiffs' and Class Members' Personal and Financial Information to Defendant's Website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

371. **Electronic Communications**. The transmission of Personal and Financial Information between Plaintiffs and Class Members and 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 photo optical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

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

373. **Interception**. The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or

other device" and "contents…include any information concerning the substance, purport, or meaning of that communication." See 18 U.S.C. § 2510(4), (8).

374. **Electronic, Mechanical or Other Device**. 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). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiffs' and Class Members' browsers;

b. Plaintiffs' and Class Members' computing devices;

c. Defendant's web-servers;

d. Defendant's Website; and

e. The tracking technology deployed by Defendant effectuated the sending and acquisition of customer communications.

375. By utilizing and embedding the tracking technology on its Website, Defendant intentionally intercepted, endeavored to intercept and procured another person to intercept the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

376. Specifically, Defendant intercepted Plaintiffs' and Class Members' electronic communications via the tracking technology which tracked, stored, and unlawfully disclosed Plaintiffs' and Class Members' Personal and Financial Information to Third Parties.

377. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiffs and Class Members regarding Personal and Financial Information.

378. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members to 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).

379. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs and Class Members, 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).

380. **Unauthorized Purpose.** Defendant intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely, invasion of privacy, among others.

381. Defendant intentionally used the wire or electronic communications to increase its profit margins and save on marketing costs.

382. Defendant specifically used tracking technology to track and to utilize Plaintiffs' and Class Members' Personal and Financial Information for financial gain.

383. Defendant was not acting under color of law to intercept Plaintiffs' and Class Members' wire or electronic communication.

384. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiffs' and Class Members' privacy via the tracking technology.

385. In sending and in acquiring the content of Plaintiffs' and Class Members' communications relating to the browsing of its Website, Defendant's purpose was tortious, criminal and designed to violate federal and state legal provisions, including as described above the following: (i) a knowing intrusion into a private, place, conversation or matter that would be

highly offensive to a reasonable person; and (ii) violation of GLBA, the FTC Act, invading Plaintiffs' and Class Members' privacy, and in breach of its fiduciary duty of confidentiality.

**COUNT XV**
**VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT**
**18 U.S.C. § 2511(3)(a)**
**UNAUTHORIZED DIVULGENCE BY ELECTRONIC COMMUNICATIONS SERVICE**
**(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

386. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

387. The ECPA statute provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

388. **Electronic Communication Service**. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Defendant's Website is an electronic communication service which provides to users thereof, customers of Defendant, the ability to send or receive electronic communications; in the absence of Defendant's Website, internet users could not send or receive communications regarding Plaintiffs' and Class Members' Personal and Financial Information.

389. **Intentional Divulgence**. Defendant intentionally designed the tracking technology and was or should have been aware that, if so configured, it could divulge Plaintiffs' and Class Members' Personal and Financial Information. Upon information and belief, Defendant's divulgence of the contents of Plaintiffs' and Class Members' communications was

contemporaneous with their exchange with Defendant's Website, to which they directed their communications.

390. Defendant divulged the contents of Plaintiffs' and Class Members' electronic communications without authorization and/or consent.

391. **Exceptions do not apply**. In addition to the exception for communications directly to an electronic communications service ("ECS")[109] or an agent of an ECS, the ECPA states that

> "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication"…"as otherwise authorized in section 2511(2)(a) or 2517 of this title; "with the lawful consent of the originator or any addressee or intended recipient of such communication;" c. "to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;" or d. "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency."

U.S.C. § 2511(3)(b).

392. Section 2511(2)(a)(i) provides: It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

393. Defendant's divulgence of the contents of Plaintiffs' and Class Members' communications to Facebook was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither:

[109] An ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

(i) a necessary incident to the rendition of Defendant's service nor (ii) necessary to the protection of the rights or property of Defendant.

394. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

395. Defendant's divulgence of the contents of Plaintiffs' and the Class Members' communications on its Website through the tracking technology was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As alleged above: (i) Plaintiffs and Class Members did not authorize Defendant to divulge the contents of their communications and (ii) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiffs and Class Members were exchanging information.

396. Moreover, Defendant divulged the contents of Plaintiffs' and Class Members' communications through tracking technology to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

397. The contents of Plaintiffs' and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

398. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages, preliminary and other equitable or declaratory relief as may be appropriate, punitive damages in an amount to be determined by a jury and a reasonable attorney's fee and other litigation costs reasonably incurred.

**COUNT XVI**
**VIOLATION OF TITLE II OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("STORED COMMUNICATIONS ACT")**
**18 U.S.C. §§ 2702, *et seq.***
**(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

399. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

400. The ECPA further provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

401. **Electronic Communication Service**. ECPA defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Defendant intentionally procures and embeds various Plaintiffs' and Class Members' Personal and Financial Information through the tracking technology used on Defendant's Website, which qualifies as an Electronic Communication Service.

402. **Electronic Storage**. ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

403. Defendant stores the content of Plaintiffs' and Class Members' communications on Defendant's Website and files associated with it.

404. When Plaintiffs or Class Members make a Website communication, the content of that communication is immediately placed into storage.

405. Defendant knowingly divulges the contents of Plaintiffs' and Class Members' communications through the tracking technology.

406. **Exceptions Do Not Apply**. Section 2702(b) of the Stored Communication Act provides that an electronic communication service provider

> "may divulge the contents of a communication—" a. "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." b. "as otherwise authorized in Section 2517, 2511(2)(a), or 2703 of this title;" c. "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;" d. "to a person employed or authorized or whose facilities are used to forward such communication to its destination;" e. "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;" f. "to the National Center for Missing and Exploited Children, in connection with a reported submission thereto under section 2258A." g. "to a law enforcement agency, if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime;" h. "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency"; or "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies Section 2523."

407. Defendant did not divulge the contents of Plaintiffs' and Class Members' communications to "addressees," "intended recipients," or "agents" of any such addressees or intended recipients of Plaintiffs and Class Members.

408. Section 2517 and 2703 of the ECPA relate to investigations by government officials and have no relevance here.

409. Section 2511(2)(a)(i) provides: It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a

provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

410. Defendant's divulgence of the contents of Plaintiffs' and Class Members' communications on its Website to Third Parties was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (i) a necessary incident to the rendition of the Defendant's services nor (ii) necessary to the protection of the rights or property of Defendant.

411. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

412. Defendant's divulgence of the contents of Plaintiffs' and Class Members' customer user communications on its Website was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As alleged above: (i) Plaintiffs and Class Members did not authorize Defendant to divulge the contents of their communications and (ii) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiffs and Class Members were exchanging information.

413. Moreover, Defendant divulged the contents of Plaintiffs' and Class Members' communications through the tracking technology to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

414. The contents of Plaintiffs' and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

415. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages, preliminary and other equitable or declaratory relief as may be

appropriate, punitive damages in an amount to be determined by a jury and a reasonable attorney's fee and other litigation costs reasonably incurred.

**COUNT XVII**
**VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT ("CFAA")**
**18 U.S.C. §§ 1030, *et seq.***
**(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

416. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

417. Plaintiffs' and the Class Members' computers and mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

418. Defendant exceeded, and continues to exceed, authorized access to Plaintiffs' and the Class Members' protected computers and obtained information thereby, in violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C).

419. Defendant's conduct caused "loss to 1 or more persons during any 1-year period… aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the secret transmission of Plaintiffs' and the Class Members' Personal and Financial Information as set forth in detail herein, which were never intended for public consumption.

420. Defendant's conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV), due to the private and personally identifiable data and content of Plaintiffs and the Class Members' Personal and Financial Information and communication being made available to Defendant and Third Parties without adequate legal privacy protections.

421. Accordingly, Plaintiffs and the Class Members are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiffs, individually, on behalf of themselves, and on behalf of all others similarly situated, prays for judgment as follows:

A. For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and Plaintiffs' counsel as Class Counsel;

B. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

C. For an award of punitive damages, as allowable by law;

D. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Personal and Financial Information and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

E. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity the type of Personal and Financial Information compromised and unlawfully disclosed to Third Parties;

F. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

G. For an Order compelling Defendant to pay for not less than three years of credit monitoring services for Plaintiffs and the Classes;

H. For an award of reasonable attorneys' fees and costs under the laws outlined above, the common fund doctrine, and any other applicable law;

I. Costs and any other expenses, including expert witness fees incurred by Plaintiffs in connection with this action;

J. Pre- and post-judgment interest on any amounts awarded; and

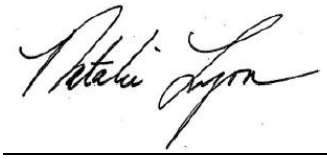
K. Such other and further relief as this court may deem just and proper.

**JURY DEMAND**

Plaintiffs, on behalf of himself, and all others similarly situated, hereby demands a trial by jury on all issues so triable.

Dated: August 26, 2024

Respectfully submitted,



Natalie Lyons, No. 293026
Vess A. Miller, No. 278020
Lynn A. Toops*
Amina A. Thomas*
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
nlyons@cohenandmalad.com
vmiller@cohenandmalad.com
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

J. Gerard Stranch, IV*
Emily E. Schiller*
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
eschiller@stranchlaw.com

Samuel J. Strauss*
Raina C. Borrelli*
STRAUSS BORRELLI, PLLC
980 N. Michigan Avenue, Suite 1610

Chicago, Illinois 60611
(872) 263-1100
(872) 263-1109 (facsimile)
sam@straussborrelli.com
raina@straussborrelli.com

*To move for *pro hac vice* admission

***Counsel for Plaintiffs and the Proposed Classes***