

1 Natalie Lyons, No. 293026
2 Vess A. Miller, No. 278020
3 Lynn A. Toops*
4 Amina A. Thomas*
5 COHEN & MALAD, LLP
6 One Indiana Square, Suite 1400
7 Indianapolis, Indiana 46204
8 Tel: (317) 636-6481
9 nlyons@cohenandmalad.com
10 ltoops@cohenandmalad.com

11 *To move for *pro hac vice* admission
12 [additional counsel listed on signature pages]

13 **Counsel for Plaintiff and Proposed Class**

14 **UNITED STATES DISTRICT COURT**
15 **NORTHERN DISTRICT OF CALIFORNIA**
16 **SAN FRANCISCO DIVISION**

17 **VISHAL SHAH, GARY INGRAHAM, DEIA**
18 **WILLIAMS, and DEVIN ROSE,**
19 **individually, and on behalf of all others**
20 **similarly situated,**

21 **Plaintiffs**

22 **v.**

23 **CAPITAL ONE FINANCIAL**
24 **CORPORATION, d/b/a CAPITAL ONE,**
25 **d/b/a CAPITAL ONE, NATIONAL**
26 **ASSOCIATION, d/b/a CAPITAL ONE, N.A.,**
27 **d/b/a CAPITAL ONE SHOPPING**

28 **Defendant.**

Civil Action No. _____

CLASS ACTION COMPLAINT FOR:

1. Negligence
2. Negligence Per Se
3. Invasion of Privacy
4. Violation of Comprehensive Computer Data Access and Fraud Act, Cal. Pen. Code § 502
5. Violation of Consumer Protection Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.*
6. Violation of Consumer Privacy Act, Cal. Civ. Code, §§ 1798.100, *et seq.*
7. Violation of Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*
8. Breach of Express and Implied Contract
9. Unjust Enrichment
10. Bailment
11. Declaratory Judgment
12. Breach of Confidence
13. Violation of Invasion of Privacy Act, Cal. Pen. Code §§ 630, *et seq.*
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.*
15. Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq.*

DEMAND FOR JURY TRIAL

1 **CLASS ACTION COMPLAINT**

2 Plaintiffs, Vishal Shah, Gary Ingraham, Deia Williams, and Devin Rose, individually, and
3 on behalf of all others similarly situated (hereinafter “Plaintiffs”) bring this Class Action
4 Complaint against Defendant, Capital One Financial Corporation, d/b/a Capital One, National
5 Association (“Capital One” or “Defendant”), and allege, upon personal knowledge as to their own
6 actions, and upon information and belief as to all other matters, as follows.
7

8 **INTRODUCTION**

9 1. Plaintiffs bring this class action to address Defendant’s outrageous, illegal, and
10 widespread practice of disclosing—without consent—the Nonpublic Personal Information¹ and
11 Personally Identifiable Financial Information² (together, “Personal and Financial Information”) of
12 Plaintiffs and the proposed Class Members to third parties, including Meta Platforms, Inc. d/b/a
13 Meta (“Facebook” or “Meta”), Google, LLC (“Google”), Microsoft Corp. (“Microsoft”),
14 DoubleClick, NewRelic, Adobe, Everest, Skai/Kenshoo, Snowplow, BioCatch, Tealium, and
15 possibly others (collectively the “Third Parties”) (in short, “the Disclosure”).
16
17

18 2. Capital One is a massive financial institution which provides financial services to
19 customers across the globe and the United States, including in California and Virginia. To provide
20 these services, Capital One operates and encourages its customers to use its website,
21

22
23 ¹ The United States Congress defines “nonpublic personal information” as “personally
24 identifiable financial information-- (i) provided by a consumer to a financial institution; (ii)
25 resulting from any transaction with the consumer or any service performed for the consumer; or
26 (iii) otherwise obtained by the financial institution.” The Gramm-Leach-Bliley Act, 15 U.S.C.A.
27 § 6809(4)(A) (“GLBA”).

28 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).

1 <https://www.CapitalOne.com> (the “Website”), on which customers can access their account
2 information, access Capital One’s financial services, and apply for financial products like credit
3 cards.
4

5 3. Despite its unique position as a massive and trusted bank, Capital One used its
6 Website to blatantly collect and disclose Consumers’³ and Customers’⁴ (collectively, “Customers”)
7 Personal and Financial Information to Third Parties uninvolved in the provision of financial
8 services—entirely without their knowledge or authorization. Capital One did so by knowingly and
9 secretly configuring and implementing code-based tracking devices (“trackers” or “tracking
10 technologies”) into its Website.
11

12 4. Through these trackers, Capital One disclosed and continues to disclose Personal
13 and Financial Information that Customers input into and accessed on Capital One’s Website. This
14 information includes without limitation account information, credit card application information,
15 and credit card pre-approval information, including the fact that a user was on a certain page, that
16 users clicked buttons and what URLs or webpages they led to, information entered on preapproval
17 application pages including their employment information, bank account information, and
18 Customers’ eligibility, preapproval, or approval for a credit card.
19

20 5. Upon information and belief, Capital One utilized data from trackers to improve
21 and to save costs on its marketing campaigns, improve its data analytics, attract new customers,
22

23
24 ³ The term “consumer” means “an individual who obtains or has obtained a financial
25 product or service from [a financial institution] that is to be used primarily for personal, family, or
26 household purposes, or that individual’s legal representative.” 16 C.F.R. § 313.3; 15 U.S.C.A. §
27 6809(9).

28 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.

1 and generate sales. Capital One benefited from use of Customers' Personal and Financial
2 Information. Capital One further allowed the Third Parties, who are uninvolved in Capital One's
3 provision of financial services, to profit from its Disclosure of Customers' Private and Financial
4 information. And the Third Parties used Customers' Personal and Financial Information for
5 themselves and disclosed to fourth parties who also profited off of it. Facebook, for example, will
6 use the data collected from Customers of Capital One to sell ads to fourth parties who will profit
7 off of the use of that information
8

9
10 6. Customers, like Plaintiffs and Class Members, simply do not anticipate that a
11 trusted financial institution will send their Personal and Financial Information to hidden Third
12 Parties (who in turn share with fourth parties), all of whom profit off of it; likewise, when Plaintiffs
13 and Class Members used Defendant's Website, they thought they were communicating exclusively
14 with a trusted financial institution.
15

16 7. At no time did Capital One disclose to Plaintiffs or Class Members that they were
17 sharing their Personal and Financial Information with the Third Parties for third- and fourth-party
18 use. Plaintiffs and Class Members never signed a written authorization permitting Defendant to
19 send their Personal and Financial Information to the Third Parties who were uninvolved in the
20 provision of financial services. And Capital One never allowed Plaintiffs or Class Members a real
21 opportunity to opt-out of its Disclosure.
22

23 8. Defendant owed a variety of duties, including common law, statutory, contractual,
24 and regulatory duties, to keep Plaintiffs' and Class Members' Personal and Financial Information
25 safe, secure, and confidential.
26
27
28

1 9. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiffs’
2 and Class Members’ Personal and Financial Information, Defendant assumed legal and equitable
3 duties to those individuals to protect and safeguard their information from unauthorized disclosure.
4

5 10. The statutory and regulatory duties Capital One owed Customers include its
6 obligations under federal law. For example, the GLBA requires that “each financial institution has
7 an affirmative and continuing obligation to respect the privacy of its customers and to protect the
8 security and confidentiality of those customers’ nonpublic personal information.” 15 U.S.C.A. §
9 6801. Under this federal law, financial institutions like Capital One are explicitly prohibited from
10 disclosing a Customer’s Personal and Financial Information without sufficient advance
11 notification and opt-out opportunity. 15 U.S.C.A. § 6801, *et seq.*
12

13 11. Capital One ignored all its duties and obligations, including the GLBA’s
14 prohibition, by disclosing Customers’ Personal and Financial Information without proper advance
15 notification and opt-out rights as required under the GLBA.
16

17 12. Examples of “Personal and Financial Information” included in the GLBA are
18 indistinguishable from the types of information Capital One disclosed to Facebook, including,
19 among other things: (a) “[i]nformation a consumer provides to [Capital One] on an application to
20 obtain a loan, credit card, or other financial product or service”; (b) “[t]he fact that an individual
21 is or has been one of [Capital One’s] customers or has obtained a financial product or service from
22 [Capital One]”; (c) “information about [Capital One’s] consumer . . . disclosed in a manner that
23 indicates that the individual is or has been [Capital One’s] consumer”; (d) “information that a
24 consumer provides to [Capital One] or that [Capital One] or [its] agent otherwise obtain[s] in
25 connection with collecting on, or servicing, a credit account”; “[a]ny information that a consumer
26 provides to [Capital One] or that [Capital One] or [its] agent otherwise obtain[s] in connection
27
28

1 with collecting on, or servicing, a credit account; and (e) “any information [Capital One] collect[s]
2 through an Internet ‘cookie’ (an information collecting device from a web server).” 16 C.F.R.
3 313.3(o)(2)(i).
4

5 13. Capital One breached its duties under California state law, including, for example,
6 the California Consumer Privacy Act. That statute provides California consumers with rights to
7 control their personal information including the right to know what personal information is being
8 collected about them and whether that information is sold or disclosed and to whom, the right to
9 prohibit the sale of their personal information, and the right to request deletion of their personal
10 information. Cal. Civ. Code § 1798.100 *et seq.* Capital One breached its obligations under this
11 statute by, for example, failing to provide Customers with appropriate notice that their information
12 was being disclosed to Third Parties for third- and fourth- party use. The notice and consent Capital
13 One purports to provide and obtain, through the policies it provides on its website, is not
14 appropriate, as a reasonable Consumer would not have understood those policies as notifying them
15 of Capital One’s disclosure of their Personal and Financial Information to Third Parties for third-
16 and fourth- party use.
17
18

19 14. Capital One breached its common law, statutory, and contractual obligations to
20 Plaintiffs and Class Members by, *inter alia*, (i) failing to adequately review its marketing programs
21 and web based technology to ensure its Website was safe and secure; (ii) failing to remove or
22 disengage technology that was known and designed to share Personal and Financial Information;
23 (iii) aiding, agreeing, and conspiring with the Third Parties to intercept communications sent and
24 received by Plaintiffs and Class Members; (iv) failing to obtain the written consent of Plaintiffs
25 and Class Members to disclose their Personal and Financial Information to Third Parties for Third
26 Party and fourth party use; (v) failing to protect Personal and Financial Information and take steps
27
28

1 to block the transmission of Plaintiffs’ and Class Members’ Personal and Financial Information
2 through the use of tracking technology; (vi) failing to warn Plaintiffs and Class Members; and (vii)
3 otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of
4 its customers’ Personal and Financial Information.
5

6 15. Plaintiffs seek to remedy these harms and brings causes of action of (I) Negligence;
7 (II) Negligence Per Se; (III) Invasion Of Privacy Cal. Const. Art. 1 § 1; (IV) Violation Of The
8 Comprehensive Computer Data Access And Fraud Act (“CDAFA”), Cal. Penal Code § 502; (V)
9 Violation Of California’s Consumer Protection Law (“UCL”), Cal. Bus. & Prof. Code §§ 17200,
10 *et seq.*; (VI) Violation of California Consumer Privacy Act (“CCPA”), 1798.100, *et seq.*; (VII)
11 Violation of The California Customer Records Act (“CRA”), Cal. Civ. Code § 1798.80, *et seq.*;
12 (VIII) Breach Of Implied Contract; (IX) Unjust Enrichment; (X) Bailment; (XI) Declaratory
13 Judgment; (XII) Breach Of Confidence; (XIII) Violation of The California Invasion of Privacy Act
14 (“CIPA”), Cal. Penal Code §§ 630, *et seq.*; (XIV) Violation of The Electronic Communications
15 Privacy Act (“ECPA”) 18 U.S.C. §§ 2511(1), *et seq.*; (XV) Violation of The Electronic
16 Communications Privacy Act (“ECPA”) 18 U.S.C. § 2511(3)(a) Unauthorized Divulgence By
17 Electronic Communications Service; (XVI) Violation Of Title II Of The Electronic
18 Communications Privacy Act (“Stored Communications Act”) 18 U.S.C. § 2702, *et seq.*; (XVII)
19 Violation of The Computer Fraud And Abuse Act (“CFAA”) 18 U.S.C. § 1030, *et seq.*.
20
21
22

23 16. Plaintiffs bring this action, individually and on behalf of all others similarly
24 situated, for damages and equitable relief.
25

26 **PARTIES**

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

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

3
4 18. Plaintiff Devin Rose is a natural person citizen of California, where he intends to
5 remain, who resides in California. Plaintiff Rose has been Capital One's customer since March
6 2024 and is a victim of Defendant's unauthorized Disclosure of Personal and Financial
7 Information.

8
9 19. Plaintiff Gary Ingraham is a natural person and citizen of California, where he
10 intends to remain, who resides in Corning, California in Tehama County. Plaintiff Ingraham was
11 Capital One's customer in April 2024 and is a victim of Defendant's unauthorized Disclosure of
12 Personal and Financial Information.

13
14 20. Plaintiff Deia Williams is a natural person and citizen of California, where she
15 intends to remain, who resides in Belmont, California. Plaintiff William was Capital One's
16 customer in 2023 and is a victim of Defendant's unauthorized Disclosure of Personal and Financial
17 Information.

18
19 21. Defendant Capital One is a stock corporation organized and existing under the laws
20 of the State of Virginia, with a principal place of business located at 1680 Capital One Dr, Mc
21 Lean, VA, 22102 - 3407, USA.⁵

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

25
26
27 ⁵See *Capital One Financial Corporation*, Virginia State Corporation Commission Clerk's
28 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.*

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

3
4 24. Capital One has corporate offices in San Francisco, California,⁷ and maintains at
5 least twelve physical locations in the state of California.⁸

6 **JURISDICTION AND VENUE**

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

11
12 26. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) because this
13 is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000,
14 exclusive of interest and costs, there are more than one hundred (100) members in the proposed
15 Classes, and at least one member of the Classes is a citizen of a state different from Defendant.

16
17 27. This Court also has subject matter jurisdiction under 28 U.S.C. § 1331 because it
18 arises under the laws of the United States. The Court has supplemental jurisdiction over Plaintiffs'
19 claims arising under state law pursuant to 28 U.S.C. § 1367.

20
21 28. Venue is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the
22 events and omissions giving rise to Plaintiffs' claims occurred in this district and continue to occur
23 in this district.

24
25
26
27 ⁷ *Corporate Offices*, CapitalOne.com, <https://www.CapitalOne.com/about/corporate-information/corporate-offices> (last visited Aug. 12, 2024).

28 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

We're in the business of keeping your money
and information safe.

As a business that relies on trust, protecting your information is just as important to us as protecting your finances. You can explore our privacy and protection policies, opt-out of email advertisements from us, and submit a data request.

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

Capital One is committed to your privacy

Our goal is to maintain your trust and confidence when handling personal and financial information about you.

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.CapitalOne.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).

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

5
6 34. “As one of the nation’s largest banks based on deposits as of December 31, 2023,”
7 Defendant “service[s] banking customer accounts through digital channels and our network of
8 branch locations, cafés, call centers and automated teller machines (‘ATMs’).”¹⁷

9
10 35. As of August 2024, Capital One offers 31 credit cards, including the Venture and
11 Venture X cards.¹⁸ For a Customer’s use of the Venture X Rewards Credit Card, Capital One
12 charges \$395 annually.¹⁹

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

17
18
19
20
21
22 ¹⁵ See *2023 Annual Report*, p. 36.

23 ¹⁶ *Id.*, p. 4.

24 ¹⁷ *Id.*, p. 4.

25 ¹⁸ See *Compare Credit Cards & Apply*, CapitalOne.com,
26 <https://www.capitalone.com/credit-cards/compare/> (last visited Aug 8, 2024) (“*Compare Credit
Cards*”).

27 ¹⁹ *Id.*

28 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*”).

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

5
 6 37. In short, Defendant encourages customers to use its “full-service” Website to access
 7 “almost everything customers can get in a traditional bank branch.”³⁴

8
 9 38. Defendant promotes the comprehensive functionality and use of its Website in
 10 service of its own goal of increasing profitability. In furtherance of that goal, Defendant purposely
 11 and secretly installed the Third Parties’ online tracking technology onto its Website to gather
 12 information about Customers.

13
 14 39. Capital One utilized the information it collected to market its services and bolster
 15 its profits by surreptitiously diverting the information to Third Parties like Facebook.

16
 17 40. But Defendant did not only collect information for its own use; Capital One also
 18 shared—and continues to share—Customers’ information, including Personal and Financial

19 ²⁴ See *Compare Credit Cards*.

20 ²⁵ See *Get Pre-Approved for a Capital One Credit Card*, CapitalOne.com,
 21 <https://www.capitalone.com/credit-cards/preapprove/> (last visited Aug. 8, 2024) (“*Get Pre-Approved*”).

22 ²⁶ See *Credit Cards*.

23 ²⁷ See *Sign in Page*, CapitalOne.com,
 24 <https://verified.capitalone.com/auth/primer?exp=card> (last visited Aug. 8, 2024) (“*Sign in Page*”).

25 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*”).

26 ²⁹ *Id.*

27 ³⁰ See *Sign in Page*.

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

31 ³² *Id.*

32 ³³ See generally the Website.

33 ³⁴ See *2023 Annual Report*, p. 3.

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

3
4 **B. Third Parties and Trackers: Collectors and Profiteers of Personal and Financial
Information**

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

8
9 42. When an individual accesses a webpage containing online tracking technology
10 from a Third Party, the trackers instantaneously and surreptitiously duplicate communications with
11 that webpage and send them to the Third Party. The information travels directly from both the
12 user’s browser and the webpage owner’s server and then on to the Third Party’s server, based off
13 instructions from the Third Party’s tracker. The communications and information transmitted via
14 these trackers are entirely in Defendant’s control; Customers trust Capital One with the information
15 they input on Capital One’s Website, and Capital One is in complete and exclusive control of its
16 Website and the data input therein. The transmission of Customers’ data only occurs on webpages
17 that contain tracking technology.

18
19 43. Online tracking technologies may not be deleted from an individual’s device; they
20 are built into a webpage, and a webpage user has no control or warning over their presence or data
21 collection. Third party trackers cause information to flow directly from the website user’s browser
22 and the website owner’s server to the Third Party itself. A webpage user cannot prevent or even
23 detect this transmission of data.

24
25 44. Accordingly, without any knowledge, authorization, or action by a user, a website
26 owner who has installed Third Party trackers is utilizing website source code to commandeer its
27
28

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

3
4 45. In this case, Defendant employed the Third Party trackers to intercept, duplicate,
5 and re-direct Plaintiffs' and Class Members' Personal and Financial Information to the Third
6 Parties contemporaneously, invisibly, and without the customer's knowledge.

7
8 46. Consequently, when Plaintiffs and Class Members visited Defendant's Websites
9 and communicated their Personal and Financial Information, that information was simultaneously
10 intercepted and transmitted to the Third Parties.

11
12 47. The Third Party trackers do not provide any substantive content on Capital One's
13 Website. Rather, their only purpose is to collect information to be used for the Third Party and
14 fourth parties' marketing and sales purposes.

15
16 48. The Facebook or Meta Pixel, for example, "tracks the people and type of actions
17 they take" on a website.³⁵ It can be used to gather customer data, identify customers and potential
18 customers, target advertisements to those individuals, and market products and services. This
19 includes when a user visits a particular webpage, clicks a button, fills out a form (including the
20 information from the form like employment information, citizenship, etcetera), IP addresses, web
21 browser information, page location, any custom events set by the website owner, the tracker ID,
22 and more.³⁶ Facebook does all of this by using the Meta Pixel to send "events" to its server.

23
24
25 ³⁵ *Retargeting*, Meta, <https://www.facebook.com/business/goals/retargeting> (last visited Aug.
26 11, 2024).

27 ³⁶ *See, e.g., Meta Pixel*, Meta for Developers, [https://developers.facebook.com/docs/meta-](https://developers.facebook.com/docs/meta-pixel/)
28 *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).

1 49. Once the data is collected via the Meta Pixel, Facebook aggregates it to build its
2 own massive, proprietary dataset, which Facebook then uses to find new customers, drive sales,
3 and understand ad impact. This is all to the benefit of the website owner, like Capital One,
4 Facebook as the third party, and other fourth parties, all of whom use the information for targeted
5 marketing campaigns. Targeting works by allowing fourth parties to direct their ads at particular
6 “Audiences,” subsets of individuals who, according to Facebook, are the “people most likely to
7 respond to your ad.”³⁷
8

9 50. Data harvesting is big business for Facebook; it drives Facebook’s advertising sales,
10 which are its profit center. In 2023, Facebook generated nearly \$135 billion in revenue, roughly
11 98% of which was derived in advertising revenue alone space.³⁸ This business model is not limited
12 to Facebook. Data harvesting one of the fastest growing industries in the country, and consumer
13 data is so valuable that it has been described as the “new oil.” Conservative estimates suggest that
14 in 2018, Internet companies earned \$202 per American user from mining and selling data. That
15 figure is only due to keep increasing; estimates for 2022 were as high as \$434 per user, for a total
16 of more than \$200 billion industry wide.
17

18 51. On information and belief, the trackers Defendant installed from other Third
19 Parties, including Google, Microsoft, DoubleClick, New Relic, Adobe, Everest, Skai/Kenshoo,
20 Snowplow, BioCatch, and Tealium, work similarly to the Meta Pixel and likewise transmitted
21 Plaintiffs’ and the Class Members’ Personal and Financial Information without Plaintiffs’ and Class
22 Members’ knowledge or authorization.
23
24

25
26 ³⁷ *Audience Ad Targeting*, Meta, <https://www.facebook.com/business/ads/ad-targeting>
27 (last visited Aug. 14, 2023).

28 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).

1 52. The Google trackers allow Defendant to track and share with Google (1) who uses
 2 Capital One’s website; (2) what is performed on the website; (3) when users visit the website; (4)
 3 where on the website users perform these actions; and (5) how users navigate through the website
 4 to perform these actions. Google gathers this information using trackers embedded on Capital
 5 One’s Website and generates corresponding reports.³⁹ DoubleClick is part of the suite Google uses
 6 to collect all of this.⁴⁰ Google’s collection of this data “enables advertisers to more effectively
 7 create, manage and grow high-impact digital marketing campaigns.”⁴¹
 8

9 53. The Microsoft tracker allows Defendant to “[t]rack what your customers are doing
 10 after they click on your ad.”⁴² According to Microsoft, the tracker “records what customers do on
 11 your website . . . [and] will collect data that allows you to track conversion goals and target
 12 audiences with remarketing lists.”⁴³
 13

14 54. The New Relic tracker is an application performance management tool, used for
 15 application monitoring, which can track every action a user performs on the website.⁴⁴
 16

17 55. The Adobe tracker can collect a veritable wealth on information on Defendant’s
 18 Website, including page views, clicks, time on page, scroll depth, video views, form submissions,
 19

20
 21 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/>.

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

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

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

28 ⁴³ *Id.*

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

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

5
6 56. The Skai/Kenshoo tracker can collect ad performance metrics like clicks,
7 impressions, click-through rates, conversions, search terms, search volume, audience data,
8 engagement metrics, and user behavior.⁴⁷

9
10 57. Snowplow is a data collection platform that allows collection and management of
11 a wide variety of data, and allows for the creations of “rich, unified customer profiles with out-of-
12 the box identity resolution.”⁴⁸

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

17
18
19
20
21
22
23 ⁴⁵ See *Audience Manager Benefits*, Adobe, <https://business.adobe.com/products/audience-manager/benefits.html> (last visited Aug. 8, 2024)

24 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).

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

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

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

28 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).

1 59. The Tealium tracker can track page views, clicks, scroll depth, form submissions,
2 video views, custom events, user information, marketing and sales data, and custom and third-
3 party data.⁵²
4

5 **C. Capital One Used Trackers to Unauthorizedly Disclose Personal and Financial**
6 **Information**

7 60. On information and belief, Capital One installed each of these trackers, through
8 which Capital One transmitted Customers' communications with Capital One's website and thus
9 their Personal and Financial Information to the Third Parties without Customers' knowledge or
10 authorization. This information included their browsing activities including the pages they viewed
11 and the buttons they clicked; information revealed in the application process regarding (i) their
12 employment, (ii) bank accounts, and (iii) Customers' eligibility, pre-approval, or approval for a
13 credit card; as well identifying information, such as IP addresses and identifying cookies.
14

15 61. On information and belief, since at least November 30, 2023, and at least as recently
16 as June 24, 2024, Capital One has tracking technologies installed on its Website. Archives also
17 show that Capital One previously configured Meta to pull information automatically from Capital
18 One's Website.
19

20 62. Accordingly, Capital One disclosed its Customers'—including Plaintiffs' and the
21 Class Members'—data and Personal and Financial Information to the Third Parties, like Facebook,
22 beginning some time prior to November 30, 2023, and at least up to June 24, 2024.
23

24 63. By way of example, as configured as of November 30, 2023, Defendant's Facebook
25 Pixel and/or its other tracking technologies, disclosed significant information to Facebook.
26
27
28

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

1 loaded, informing Facebook that the user was learning about “Cash Back Credit Cards | Capital
2 One”:

3

4 **Demonstrative 11/30/2023 Meta Pixel Configuration**

5

6

7

8

9

10

11

12

13

14

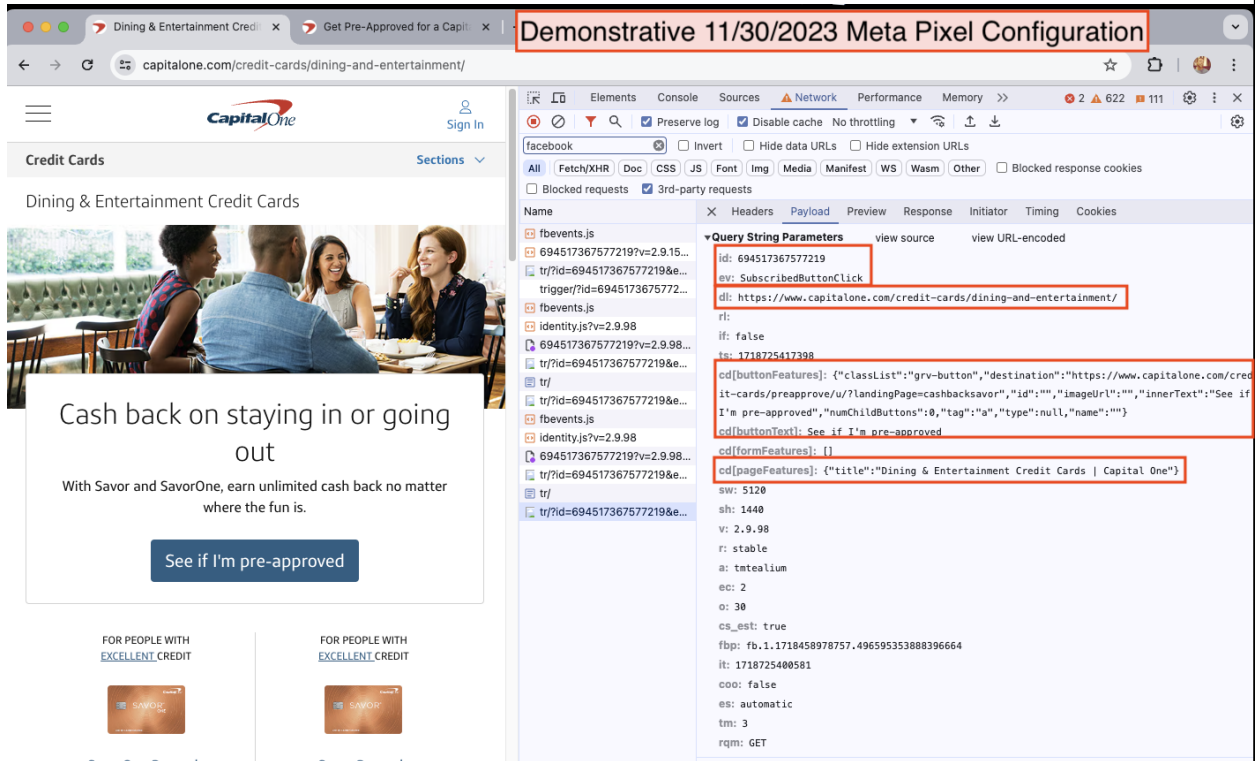
15 66. Then, if the user clicked to learn about credit cards that provide cash back on dining
16 and entertainment, Capital One would send an event via the tracker informing Facebook of this
17 activity.

18

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

24

25 68. If the user then clicked to “See if I’m pre-approved,” Capital One would send an
26 event informing Facebook about the user’s activity. The event reveals that the user clicked to go
27 to “credit-cards/preapprove/u/?landingPage=cashbacksavor” to apply for pre-approval.
28



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.

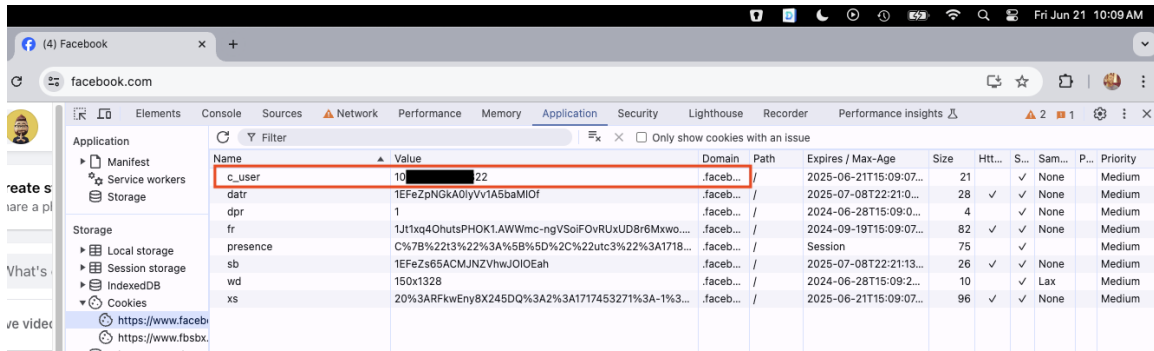
71. Furthermore, in each of the Meta Pixel events that Capital One sends to Facebook, Capital One includes a cookie which Facebook uses to identify users. Facebook can therefore

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*

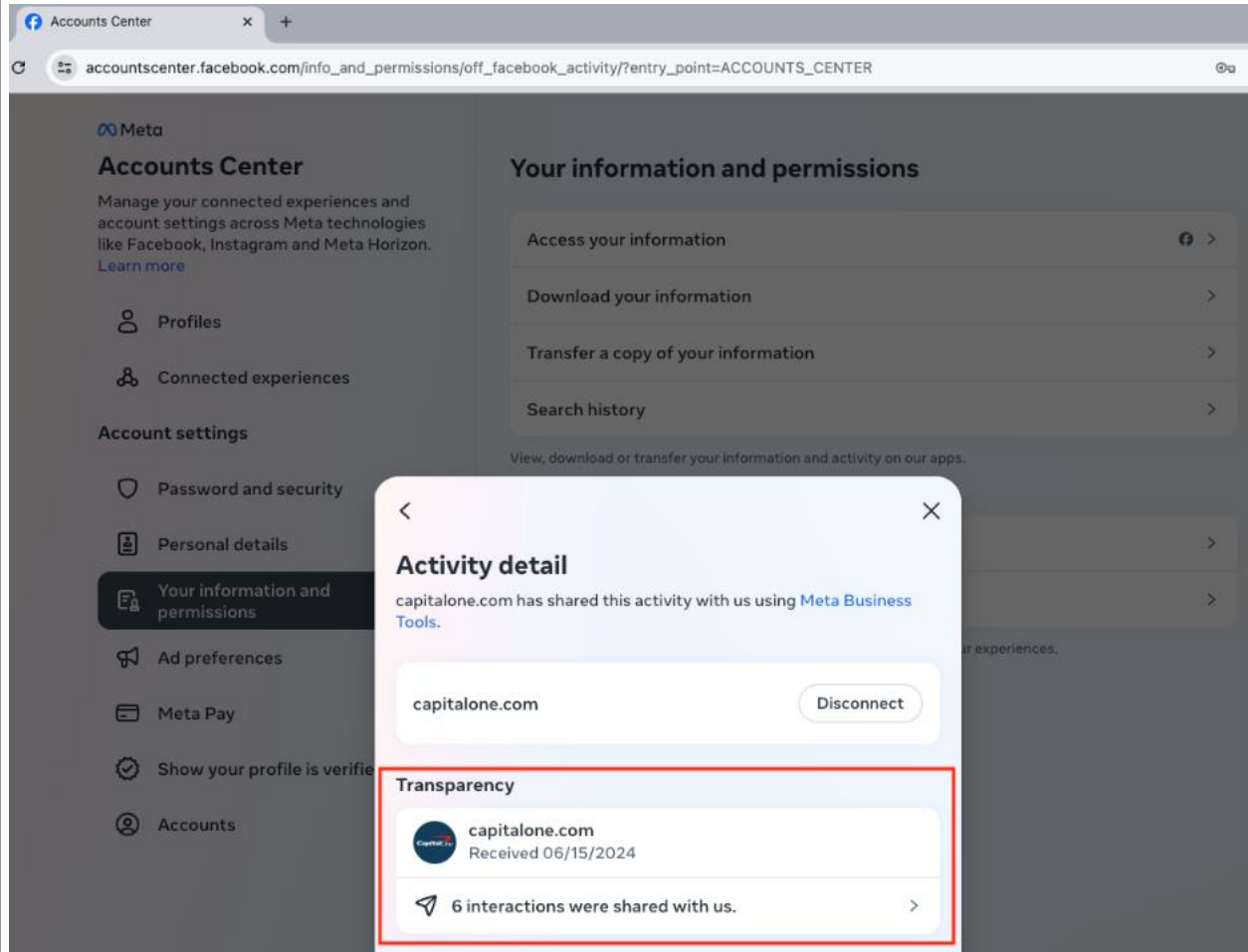
72. Defendant also disclosed Customers’ identifying information, including their IP addresses and identifying cookies, and/or Facebook ID.

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

1 profit purposes. Customers were never provided with any written notice that Defendant disclosed
 2 their Personal and Financial Information to Third Parties (who then allowed fourth parties to use
 3 it for profit), nor were they provided means of opting out of such disclosures.
 4

5 78. Customers relied on Defendant to keep their Personal and Financial Information
 6 confidential and securely maintained and to use this information only for the purpose of providing
 7 legitimate financial services. Customers relied on Defendant to make only authorized disclosures
 8 of this information.
 9

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

12 80. The contracts that Capital One has with its Customers include "Our Privacy
 13 Protections",⁵³ "Online Privacy Policy,"⁵⁴ "U.S. Consumer Privacy Notice,"⁵⁵ "Manage Your
 14 Data",⁵⁶ "California Consumer Privacy Act Disclosure,"⁵⁷ and "Social Security Number
 15 Protections,"⁵⁸ (collectively, "Privacy Contracts").
 16

17 81. "The Capital One Online Privacy Policy includes information for everyone about
 18 [Capital One's] online information practices."⁵⁹ Capital One promises that it is "in the business of
 19
 20

21 _____
 22 ⁵³ *Our Privacy Protections*, <https://www.capitalone.com/privacy/> (last visited Aug. 13,
 2024) (Exhibit A).

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

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

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

28 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/](https://www.capitalone.com/privacy/social-security-number/) (Exhibit F).

⁵⁹ *Our Privacy Protections* (Exhibit A).

1 keeping your money and information safe.”⁶⁰ But Capital One fails to keep Customers’ information
 2 safe, instead disclosing it to Third Parties (and eventually fourth parties) uninvolved in providing
 3 financial services to Plaintiffs and Class Members without Customers’ authorization or consent.
 4

5 82. “As a business that relies on trust, protecting your information is just as important
 6 to us as protecting your finances,” Capital One tells Customers.⁶¹ But despite recognizing its
 7 elevated position as trusted provider of financial services, Capital One fails to live up to that
 8 expectation by failing to protect the privacy of its Customers’ information.
 9

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

11 83. “The U.S. Consumer Privacy Notice applies to customers, applicants, and former
 12 customers of the Capital One family of companies listed in the notice.”⁶² “It details [Capital One’s]
 13 privacy and security practices regarding [its] relationship with [Customers] and provides
 14 instructions on how to limit the sharing of [Customers’] information.”⁶³
 15

16 84. This notice recognizes that, under federal law, Customers may limit “sharing for
 17 nonaffiliates to market to” them.⁶⁴ Capital One’s U.S. Consumer Privacy Notice represents:

18 Federal law also requires us to tell you how we collect, share, and protect your
 19 personal . . . The types of personal information we collect and share depend on the
 20 product or service you have with us. This information can include:

- 21 • Social Security number and income
- 22 • Account balances and payment history
- 23 • Account transactions and credit card or other debt⁶⁵

24 85. But the types of personal information that Capital One collects and shares does *not*
 25 depend on the product or service a Customer has with it. Instead, Capital One indiscriminately
 26

26 ⁶⁰ *Id.*

27 ⁶¹ *Id.*

28 ⁶² *Id.*

⁶³ *Id.*

⁶⁴ *U.S. Consumer Privacy Notice* (Exhibit C).

⁶⁵ *Id.*

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

3
4 86. Capital One “list[s] the reasons financial companies can share their customers’
5 personal information; the reasons Capital One chooses to share; and whether you can limit this
6 sharing.”⁶⁶ Those reasons include “our everyday business purposes-such as to process your
7 transactions, maintain your accounts(s), respond to court orders and legal investigations, or report
8 to credit bureaus”; “For our marketing purposes – to offer our products and services to you”; “For
9 joint marketing with other financial companies”; “For our affiliates’ everyday business purposes –
10 information about your transactions and experiences”; “For our affiliates’ everyday business
11 purposes – information about your creditworthiness”; “For our affiliates to market to you”; and
12 “For our nonaffiliates to market to you.”⁶⁷

13
14 87. The U.S. Consumer Privacy Notice defines an Affiliate as “Companies related by
15 common ownership or control. They can be financial and nonfinancial companies.”⁶⁸ Joint
16 marketing is “A formal agreement between nonaffiliated financial companies that together market
17 financial products or services to [Customers].”⁶⁹ Capital One’s “joint marketing partners include
18 companies such as other banks and insurance companies.”⁷⁰ Certainly, Third Parties like Facebook
19 do not meet either of these definitions. Capital One finally defines “nonaffiliates,” which are
20 “Companies not related by common ownership or control.”⁷¹ “They can be financial and
21 nonfinancial companies.”⁷² Capital One identifies the types of “[n]onaffiliates we share with”
22
23
24

25 ⁶⁶ *Id.*

26 ⁶⁷ *Id.*

27 ⁶⁸ *Id.*

28 ⁶⁹ *Id.*

⁷⁰ *Id.*

⁷¹ *Id.*

⁷² *Id.*

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

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

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

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

26 ⁷³ *Id.*

27 ⁷⁴ Like Capital One, Third Parties like Facebook may include advertisements on their
28 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.

1 91. By always exercising its discretion in its own favor and to the detriment of
2 Customers, Defendant breaches the reasonable expectations of Customers and, in doing so,
3 violates its duty to act in good faith.
4

5 *ii. The Online Privacy Policy*

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

8 93. Capital One states in its Online Privacy Policy that it “may collect information”
9 both directly from Customers and automatically when they use Capital One’s Website.⁷⁶ The
10 Privacy Policies explain:
11

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

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

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

26
27 ⁷⁵ See *Online Privacy Policy* (Exhibit B).

28 ⁷⁶ *Id.*

⁷⁷ *Id.*

⁷⁸ *Id.*

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

3
4 96. The Online Privacy Policy provides a final, catch-all category, which permits
5 Capital One to “share *aggregated and de-identified information* (such as aggregated statistics
6 regarding the use of our financial products and services) with third parties for any purpose.”⁷⁹

7
8 97. The Online Privacy Policy thus makes clear that, if Capital One desires to share
9 Customers’ Personal and Financial Information with a Third Party like Facebook, such information
10 cannot contain any details linking it to specific Customers. Rather, the information may be shared
11 only in an “aggregated and de-identified” form.

12
13 98. Capital One violates this agreement by sharing Customers’ Personal and Financial
14 Information with Third Parties in a manner that is neither aggregated nor de-identified. To the
15 contrary, Capital One routinely shares Customers’ Personal and Financial Information in a format
16 that enables the Third Parties to identify and target specific Customers.

17
18 99. Capital One’s Online Privacy Policy also enumerates and exemplifies the purposes
19 for which Capital One may use Customer information. Such purposes include:

20 **Providing our products and services**, such as enabling you to apply for and obtain
21 Capital One products or services, evaluating your application or eligibility for a
22 Capital One product or service, servicing and managing your accounts, providing
23 customer service or support, communicating with you, and providing online tools
24 and features.

25 **Processing transactions and payments**, such as transferring funds between
26 accounts, processing payments or transactions, fulfilling orders, and conducting
27 settlement, billing, processing, clearing, or reconciliation activities, and helping
28 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).

1 **Detecting and preventing fraud**, such as determining fraud risk and identifying
2 fraudulent transactions.

3 **Protecting against security risks**, such as monitoring network activity logs,
4 detecting security incidents, conducting data security investigations, and otherwise
5 protecting against malicious, deceptive, fraudulent, or illegal activity.

6 **Advertising and marketing**, such as sending you offers for special products and
7 services via mail, email, or text message, displaying online advertising, targeting
8 our offers or promotions, providing sweepstakes, conducting market research, and
9 evaluating or improving the effectiveness of our marketing efforts. Learn more
10 about how we use online tracking technology.

11 **Conducting analytics and research**, such as examining which parts of our website
12 you visit or which aspects of our mobile apps you find most useful, evaluating user
13 interface and experiences, testing features or functionality, performing debugging
14 and error repair, and analyzing the use of our Online Services. Learn more about
15 how we use online tracking technology.

16 **Improving our products and services**, such as personalizing and optimizing your
17 website and mobile experiences, recognizing you across different browsers and
18 devices you use, improving existing products and services, and developing new
19 products and services.

20 **Carrying out legal and business purposes**, such as complying with applicable
21 laws, responding to civil, criminal, or regulatory lawsuits, subpoenas, or
22 investigations, exercising our rights or defending against legal claims (including
23 for collections and recoveries on past-due accounts), resolving complaints and
24 disputes, performing compliance activities, analyzing credit risk, conducting credit
25 reporting activities, regulatory reporting, performing institutional risk control,
26 conducting human resources activities, and otherwise operating, managing, and
27 maintaining our business.

28 **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.*

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

3
4 101. Capital One again explains the groups with and context in which it “may” share
5 this collected information:

6 **Affiliates.** We may share information with companies in the Capital One family.

7 **Business partners.** We may share information with companies that we have
8 partnered with to offer or enhance products and services for Capital One customers
9 or prospective customers. For example, we may share information with co-branded
10 credit card partners, joint marketing partners, bill pay partners, or retail partners
11 that allow you to redeem credit card rewards.

12 **Marketing partners.** We may allow companies to collect information through our
13 Online Services in order to provide marketing services to us, including to target
14 advertising to you based on personal information collected across different
15 websites, mobile apps, and devices over time. Learn more about how we use online
16 tracking technology to conduct personalization, analytics, and targeted advertising,
17 and how you can opt out.

18 **Service providers.** We use other companies to provide services on our behalf and
19 to help us run our business. We may share information with these service providers,
20 or they may collect information on our behalf, for various business purposes. For
21 example, we use service providers for hosting and securing our information
22 systems, servicing customer accounts, detecting and preventing fraud, assisting
23 with human resources activities, communicating with our customers, and analyzing
24 and improving our Online Services.

25 **Other third parties with your consent or as necessary to provide our products
26 and services.** We share information with your consent or at your direction, such as
27 when you ask us to share information with a money management app to track your
28 finances or 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).

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

9
10
11 107. Thus, the Online Privacy Policy’s discussion of cookies or pixels does not apply to
12 the collection or disclosure of information to Third Parties or their trackers for targeted advertising
13 on their platforms (and fourth party platforms).

14
15 108. Capital One’s disclosure of its use of “Pixel tags” further does not apply to the Third
16 Parties because the Third Parties are not “service providers,” as required in that provision.

17 109. The “Pixel tags” disclosure states:

18 **Pixel tags.** A pixel tag (also known as a web beacon, clear GIF, pixel, or tag) is an
19 image or a small string of code that may be placed in a website, advertisement, or
20 email. It allows companies to set or read cookies or transfer information to their
21 servers when you load a webpage or interact with online content. For example, *we*
22 *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

23 110. This language limits the entities that can use pixel tags to Capital One and its
24 “service providers.” The Online Privacy Policy defines a service provider as “other companies
25 [that] provide services *on our behalf and to help us run our business*...[T]hey may collect
26

27
28 ⁸⁵ *Id.* (emphasis added).

⁸⁶ *Id.* (emphasis added).

⁸⁷ *Id.* (bolded italics added).

1 information *on our behalf, for various business purposes.*⁸⁸ “For example, we use service
2 providers for hosting and securing our information systems, servicing customer accounts, detecting
3 and preventing fraud, assisting with human resources activities, communicating with our
4 customers, and analyzing and improving our Online Services.”⁸⁹ Third Party use of Customer data
5 for Third Party and fourth party advertisement does not fall within these definitions and therefore
6 is not permitted by the Online Privacy Policy.
7

8 111. Further, like the U.S. Consumer Privacy Notice, Capital One’s Online Privacy
9 Policy grants Capital One sole discretion to share Customers’ Personal and Financial Information,
10 stating: “We *may* share information in a variety of contexts.”⁹⁰
11

12 112. Customers reasonably understand that Capital One will securely maintain their
13 Personal and Financial Information entrusted to it and protect the information from being shared
14 or utilized by Third Parties (and fourth parties) that have nothing to do with Capital One or its
15 services. Capital One’s Online Privacy Policy only reinforced this reasonable understanding.
16

17 113. Nevertheless, Capital One abuses its contractual discretion it reserved wholly for
18 itself and acts in a manner that it knows to be inconsistent with its Customers’ reasonable
19 expectations under its Online Privacy Policy.
20

21 114. By always exercising its discretion in its own favor and to the prejudice of
22 Customers, Defendant breaches the reasonable expectations of Customers and, in doing so,
23 violates its duty to act in good faith.
24
25
26

27 ⁸⁸ *Id.* (emphasis added).

28 ⁸⁹ *Id.*

⁹⁰ *Id.* (emphasis added).

1 iii. *The California Consumer Privacy Act Disclosure*

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

5
6 116. The California Consumer Privacy Act Disclosure limits Capital One’s ability to
7 share information with “other third parties” to entities such as “[p]ayment processors, merchants,
8 or other financial institutions” and, even then, sharing is limited to instances where Customers
9 consent or “as necessary to provide *our* products and services.”⁹²

10
11 117. Capital One and its California Customers thus agreed that Capital One may share
12 their Personal and Financial Information with nonaffiliated third parties only if the Customer
13 expressly consented or, where “necessary,” for the limited purpose of providing *Capital One’s*
14 products and services.

15
16 118. Instead of keeping the promises in its California Consumer Privacy Act Disclosure,
17 Capital One indiscriminately shares Personal and Financial Information with nonaffiliated Third
18 Parties, without Customers’ consent and for Third Party and fourth party marketing purposes that
19 have nothing to do Capital One servicing the Customer’s account.

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

22 119. Capital One’s failure to safeguard the privacy of Customers’ Personal and Financial
23 Information as agreed in its Privacy Policies is even more egregious here, as Capital One also fails
24 to provide Customers with sufficient opportunity to opt out of disclosure to nonaffiliates (or any
25 other party, for that matter). This is because, as described above, while the U.S. Consumer Privacy
26

27
28

⁹¹ *U.S. Consumer Privacy Notice* (Exhibit C).

⁹² *California Consumer Privacy Act Disclosure* (Exhibit E) (emphasis added).

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

5
6 120. As Capital One’s Online Privacy Policy explains, Customers can “opt out of certain
7 targeted advertising” but “your preferences will apply only to the specific browser or device from
8 which you opt out.”⁹³ Customers are left with no way to fully opt out of Third Party disclosures
9 and targeted advertising. In this way, Capital One not only fails to provide Customers with
10 appropriate opportunity to opt out, but also fails to abide by its Customers’ opt out requests as
11 agreed in the U.S. Consumer Privacy Notice.

12
13 121. Capital One directs Customers to its “Google Analytics on our Online Services,”
14 and provides an “opt out” link.⁹⁴ But as discussed above, this both fails to provide Customers with
15 actual opportunity to opt out, and fails to abide by the opt out request, since Third Party trackers
16 will continue to instantaneously send data from Customers visiting Capital One’s Website.
17 Customers have **no** option to fully opt out.

18
19 122. Similarly, Capital One purports to allow Customers to “Manage [Thei]r Data.”⁹⁵
20 Capital One tells Customers: “we use data to: Service your accounts and improve your
21 experience[;] Personalize offers and services[;] Verify your identity to protect you from fraud[;]
22 and] Comply with state and federal regulations.”⁹⁶ But Capital One offers limited options to
23
24
25
26

27 ⁹³ *Online Privacy Policy* (Exhibit B).

28 ⁹⁴ *Id.*

⁹⁵ *Manage Your Data* (Exhibit D).

⁹⁶ *Id.*

1 “manage your data”—Customers may download a copy of their data, request Capital One correct
2 data, or request Capital One delete data.⁹⁷

3
4 123. Again, these options do not sufficiently allow Customers to opt-out of Capital One’s
5 data collection and Disclosure through third party tracking technology. Furthermore, these
6 promises are nothing but a sham; even when a Customer requests Capital One delete their data, in
7 **949 out of 953** instances, Capital One finds a reason **not** to do so.⁹⁸ That equates to a 0.4% chance
8 that Capital One **will** delete data when requested; inversely, there is a 99.6% chance that Capital
9 One **will not** delete data when requested.⁹⁹

10
11 124. Capital One’s privacy policies as they were in place in January 2020 are
12 substantially the same as they are now.¹⁰⁰

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

14 125. As a financial institution, Capital One is subject to the GLBA. 15 U.S.C. §
15 6809(3)(A) (a “financial institution” is “any institution the business of which is engaging in
16 financial activities...”). Defendant recognizes this, noting, “[f]or example, at the federal level, we
17 are subject to the GLBA . . . among other laws and regulations . . . Additionally, the Federal
18 Banking Agencies, as well as the SEC and related self-regulatory organizations, regularly issue
19

20
21
22
23
24 ⁹⁷ *Id.*

25 ⁹⁸ *2023 Transparency Report*, Capital One, <https://mydata.capitalone.com/transparency-report> (last visited Aug. 13, 2024).

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

27 ¹⁰⁰ See *Capital One U.S. English Privacy Opt Out Notice* (June 2020), CapitalOne.com,
28 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>.

1 guidance regarding cybersecurity that is intended to enhance cyber risk management among
2 financial institutions.”¹⁰¹

3
4 126. Pursuant to the GLBA, “each financial institution has an affirmative and continuing
5 obligation to respect the privacy of its customers and to protect the security and confidentiality of
6 those customers’ nonpublic personal information.” 15 U.S.C. § 6801(a).

7
8 127. The FTC has interpreted Section 5 of the FTC Act, 15 U.S.C. § 45, to include
9 compliance with the GLBA Privacy Rule, 16 C.F.R. § 313.1 *et seq.* The FTC consistently enforces
10 the GLBA Privacy Rule, as failure to comply with the GLBA Privacy Rule is an unfair act or
11 practice prohibited by Section 5 of the FTC Act.¹⁰²

12
13 128. The GLBA Privacy Rule is a regulation that “governs the treatment of nonpublic
14 personal information about consumers by the financial institutions.” 16 C.F.R. § 313.1 *et seq.*

15
16 129. Pursuant to the GLBA Privacy Rule, “[a] financial institution must provide a notice
17 of its privacy policies and practices with respect to both affiliated and nonaffiliated third parties,
18 and allow the consumer to opt out of the disclosure of the consumer’s nonpublic personal
19 information to a nonaffiliated third party if the disclosure is outside of the exceptions.”¹⁰³ Capital
20 One consistently fails to do this.

21
22 130. The GLBA Privacy Rule, defines sensitive information that should not be
23 indiscriminately disclosed:

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

25 ¹⁰¹ See *2023 Annual Report*.

26 ¹⁰² See *How to Comply with the Privacy Rule*, [https://www.ftc.gov/business-](https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act)
27 [guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-](https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act)
28 [bliley-act](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/](https://www.ftc.gov/legal-library/browse/rules/financial-privacy-rule)
financial-privacy-rule (last visited August 8, 2024).

1 (ii) Any list, description, or other grouping of consumers (and
2 publicly available information pertaining to them) that is derived
3 using any personally identifiable financial information that is not
publicly available....

4 (3) Examples of lists—

(i) Nonpublic personal information includes any list of individuals'
5 names and street addresses that is derived in whole or in part using
6 personally identifiable financial information (that is not publicly
available), such as account numbers....

7 (o) (1) Personally identifiable financial information means any information:

(i) A consumer provides to you to obtain a financial product or
8 service from you;

(ii) About a consumer resulting from any transaction involving a
9 financial product or service between you and a consumer; or

(iii) You otherwise obtain about a consumer in connection with
10 providing a financial product or service to that consumer.

11 (2) Examples—

(i) Information included. Personally identifiable financial
12 information:

(A) Information a consumer provides to you on an
13 application to obtain a loan, credit card, or other financial
14 product or service;

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

(C) The fact that an individual is or has been one of your
16 customers or has obtained a financial product or service from
17 you;

(D) Any information about your consumer if it is disclosed
18 in a manner that indicates that the individual is or has been
19 your consumer;

(E) Any information that a consumer provides to you or that
20 you or your agent otherwise obtain in connection with
21 collecting on, or servicing, a credit account;

(F) Any information you collect through an Internet
22 “cookie” (an information collecting device from a web
23 server); and

(G) Information from a consumer report.
24

25 16 C.F.R. § 313.3

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

1 tracker ID (which identified to each Third Party that the user that was interacting with Capital
2 One’s financial services platform); the URL of the pages visited (which disclosed the financial
3 services the user was obtaining); and the “clicks” the user made on Capital One’s website (which
4 is information Capital One obtained from the Customer in connection with providing financial
5 products and services)—is “nonpublic personal information” under the GLBA and related
6 regulations. 16 C.F.R. § 313.3.
7

8 132. Capital One has utterly failed to meet its privacy obligations under the GLBA: it
9 has explicitly disclosed Customers’ nonpublic personal information and Personal and Financial
10 Information to Third Parties for marketing and advertisement, including for Third Party and fourth
11 party advertising use, and refused to allow customers to meaningfully limit this sharing.¹⁰⁴
12

13 133. Capital One fails to meet its notice obligations under the GLBA. “[A] financial
14 institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any
15 nonpublic personal information, unless such financial institution provides or has provided to the
16 consumer a notice that complies with section 6803 of this title.” 15 U.S.C.A. § 6802. As outlined
17 at length above, Capital One’s Privacy Policies fail to put Customers on notice as required here
18 and actually promise that Customers’ Personal and Financial Information will not be shared with
19 Third Parties (and fourth parties) for targeted advertising purposes.
20

21 134. For example, by not including in its Privacy Policies that it discloses Customers’
22 Personal and Financial Information to Third Parties for their use in their own advertising and
23 marketing, the Privacy Policies fail to properly disclose:
24

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

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

1 practices of the institution with respect to disclosing of nonpublic personal
2 information of persons who have ceased to be customers of the financial
3 institution . . .

4 (2) the categories of nonpublic personal information that are collected by the
5 financial institution; [and]

6 (3) the policies that the institution maintains to protect the confidentiality and
7 security of nonpublic personal information

8 15. U.S.C.A. § 6803.

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

14 may not disclose nonpublic personal information to a nonaffiliated third party
15 unless—

16 (A) [it] clearly and conspicuously discloses to the consumer. . . that such
17 information may be disclosed to such third party;

18 (B) ***the consumer is given the opportunity***, before the time that such
19 information is initially disclosed, ***to direct that such information not be
20 disclosed to such third party***; and

21 (C) the consumer is given an explanation of how the consumer can exercise
22 that nondisclosure option.

23 15 U.S.C.A. § 6802 (emphasis added).

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

27 137. Capital One further fails to meet its opt out obligations because Customers are not
28 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.

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

3
4 139. Capital One still further fails to meet its opt out obligations because it fails to
5 provide Customers with reasonable means of opting out. The GLBA Privacy Rule provides
6 “examples of reasonable opportunity to opt out”:

7 (i) By mail. You mail the notices required in paragraph (a)(1) of this section to the
8 consumer and allow the consumer to opt out by mailing a form, calling a toll-free
9 telephone number, or any other reasonable means within 30 days from the date you
10 mailed the notices.

11 (ii) By electronic means. A customer opens an on-line account with you and agrees
12 to receive the notices required in paragraph (a)(1) of this section electronically, and
13 you allow the customer to opt out by any reasonable means within 30 days after the
14 date that the customer acknowledges receipt of the notices in conjunction with
15 opening the account.

16 (iii) Isolated transaction with consumer. For an isolated transaction, such as the
17 purchase of a money order by a consumer, you provide the consumer with a
18 reasonable opportunity to opt out if you provide the notices required in paragraph
19 (a)(1) of this section at the time of the transaction and request that the consumer
20 decide, as a necessary part of the transaction, whether to opt out before completing
21 the transaction.

22 16 C.F.R. § 313.10.

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

27 141. Capital One further fails to comply with its opt out obligations because it fails to
28 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).

1 which you opt out.”¹⁰⁶ Third Party trackers will continue to instantaneously send data from
2 Customers visiting Capital One’s Website. Customers have **no** option to fully opt out of
3 Disclosures to Third Parties or targeted advertising.
4

5 142. Capital One further fails to comply with its opt out obligations by providing
6 Customers with an “opt out” link for its use of “Google Analytics on our Online Service.”¹⁰⁷ But
7 as discussed above, this both fails to provide Customers with actual opportunity to opt out, and
8 fails to abide by the opt out request, since Third Party trackers will continue to instantaneously
9 send data from Customers visiting Capital One’s Website. Customers have **no** option to fully opt
10 out.
11

12 143. By perpetually disclosing its customers’ Personal and Financial Information to third
13 parties without consent, Capital One failed and continues to fail to meet its obligations under the
14 GLBA, FTC standards, and related regulations, to establish appropriate standards and safeguards
15 relative to Customers’ Personal and Financial Information.
16

17 **F. Plaintiffs’ Experiences**

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

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

20 146. Plaintiff Shah further applied for Defendant’s services on approximately January
21 24, 2023, when he applied for the Capital One Venture X credit card.
22

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

24 148. During the last three years, Plaintiff Shah accessed his financial information
25 maintained by Capital One through Capital One’s Website.
26

27
28 ¹⁰⁶ *Id.*

¹⁰⁷ *Id.*

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

3
4 150. Plaintiff Shah has used Capital One's Website to facilitate his financial services
5 with Defendant since February 2023 and inputted Personal and Financial Information into
6 Defendant's Website at Defendant's direction and encouragement. .

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

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

9
10 153. Shortly after Plaintiff Shah used Defendant's Website to apply for his Capital One
11 Venture X card, advertisements from NerdWallet, advertising random credit cards, began
12 appearing in his Facebook feed.

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

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

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

18 157. Plaintiff Rose has been Defendant's customer since March 2024, when he applied
19 for the Capital One Venture One credit card.
20

21 158. Plaintiff Rose was approved for the Capital One Venture One credit card and has
22 used the card at least in California since being approved.
23

24 159. Plaintiff Rose has used Capital One's Website to facilitate his financial services
25 with Defendant since March 2024 and inputted Personal and Financial Information into
26 Defendant's Website at Defendant's direction and encouragement.
27

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

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

2 162. Shortly after Plaintiff Rose used Defendant's Website to apply for his Capital One
3 Venture One credit card, Capital One credit card advertisements began appearing in his Facebook
4 feed.
5

6 163. At approximately the same time, advertisements from other credit cards and for
7 personal and business loans began appearing in Plaintiff Rose's Facebook feed.
8

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

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

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

12 167. Plaintiff Ingraham used Capital One's Website to apply for a credit card and
13 inputted Personal and Financial Information into Defendant's Website at Defendant's direction and
14 encouragement
15

16 168. Plaintiff Ingraham is a Facebook user.

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

19 170. At approximately the same time, advertisements from Chase Credit began
20 appearing in Plaintiff Ingraham's Facebook feed.
21

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

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

25 173. Plaintiff Williams applied for a Capital One Venture card in 2023 and inputted
26 Personal and Financial Information into Defendant's Website at Defendant's direction and
27 encouragement.
28

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

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

3 176. Plaintiff Williams is a Facebook user.

4
5 177. Shortly after Plaintiff Williams used Defendant's Website to apply for a Capital One
6 credit card, she was constantly bombarded with credit card advertisements on Facebook.

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

9
10 179. Plaintiffs accessed Defendant's Website at Defendant's direction and
11 encouragement.

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

15
16 181. At no point did Customers like Plaintiffs sign any written authorization permitting
17 Defendant to send their Personal and Financial Information to Third Parties (or fourth parties)
18 uninvolved in providing them with financial services.

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

23
24 183. Plaintiffs provided their Personal and Financial Information to Defendant and
25 trusted that the information would be safeguarded according to Capital One's promises and the
26 law.

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

3
4 185. Plaintiffs never intended to let Capital One benefit from their Personal and
5 Financial Information.

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

9
10 187. On information and belief, through its use of Third Party trackers on its Website,
11 Defendant disclosed to Third Parties information Plaintiffs provided to Capital One as a financial
12 institution and resulting from a transaction for Plaintiffs to obtain Defendant's credit card,
13 including each Plaintiffs':

- 14 a. Employment information;
- 15 b. Bank account information (including, at a minimum, types of bank accounts);
- 16 c. Citizenship and dual citizenship status;
- 17 d. Credit card preapproval or eligibility;
- 18 e. Credit card approval or eligibility;
- 19 f. Plaintiffs' existing user, or Customer, status;
- 20 g. Browsing activities, including the pages and content Plaintiffs viewed;
- 21 h. That Plaintiffs were applying for a credit card (their status as a Customer); and
- 22 i. Information collected through an Internet "cookie" (or information collecting
23 device from a web server).

24
25
26 188. By failing to receive the requisite consent, Capital One breached confidentiality and
27 unlawfully disclosed Plaintiffs' Personal and Financial Information.
28

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

3
4 190. As a result of Capital One's Disclosure of Plaintiffs' Personal and Financial
5 Information via the Facebook Pixel and other tracking technologies to Third Parties (and fourth
6 parties) without authorization, Plaintiffs suffered the following injuries:

- 7 a. Loss of privacy; unauthorized disclosure of their Personal and Financial
8 Information; unauthorized access of their Personal and Financial Information by
9 Third Parties;
- 10
11 b. Capital One benefited from the use of Plaintiffs' Personal and Financial
12 Information without sharing that benefit with Plaintiffs;
- 13
14 c. Plaintiffs now receive targeted advertisements from fourth parties on social media,
15 reflecting their Personal and Financial Information that was improperly disclosed
16 and used;
- 17
18 d. Plaintiffs paid Capital One for financial services, and the services they paid for
19 included reasonable privacy and data security protections for their Personal and
20 Financial Information, but due to Defendant's Disclosure, Plaintiffs did not receive
21 the privacy and security protections for which they paid;
- 22
23 e. The portion of Capital One's revenues and profits attributable to collecting
24 Plaintiffs' Personal and Financial Information without authorization and sharing it
25 with Third Parties (and fourth parties);
- 26
27 f. The portion of Capital One's savings in marketing costs attributable to collecting
28 Plaintiffs' Personal and Financial Information without authorization and sharing it
with Third Parties (and fourth parties);

- 1 g. The portion of Capital One’s revenues and profits attributable to serving and
2 monetizing advertisements directed to Plaintiffs as a result of collecting Plaintiffs’
3 Personal and Financial Information without authorization and sharing it with Third
4 Parties (and fourth parties);
- 5
- 6 h. Value to Plaintiffs of surrendering their choice to keep their Personal and Financial
7 Information private and allowing Capital One to track their data;
- 8
- 9 i. Embarrassment, humiliation, frustration, and emotional distress;
- 10 j. Decreased value of Plaintiffs’ Personal and Financial Information;
- 11 k. Lost benefit of the bargain;
- 12 l. Increased risk of future harm resulting from future use and disclosure of their
13 Personal and Financial Information; and
- 14 m. Statutory damages.
- 15

16 **TOLLING, CONCEALMENT, AND ESTOPPEL**

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

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

24 193. Plaintiffs and Class Members could not with due diligence have discovered the full
25 scope of Capital One’s conduct, because there were no disclosures or other indication that they
26
27
28

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

3
4 194. All applicable statutes of limitation have also been tolled by operation of the
5 discovery rule and the doctrine of continuing tort. Capital One's illegal interception and disclosure
6 of Plaintiffs' and the Class's Personal and Financial Information has continued unabated. What is
7 more, Capital One was under a duty to disclose the nature and significance of its data collection
8 practices but did not do so. Capital One is therefore estopped from relying on any statute of
9 limitations defenses.
10

11 **CLASS ACTION ALLEGATIONS**

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

14 196. Plaintiffs seek to represent the following classes:

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

18 **California Subclass:** All individuals in California whose Personal and Financial
19 Information was disclosed by Defendant to Third Parties through Defendant's
20 Website's tracking technology without authorization.

21 197. Excluded from the Classes are the following individuals and/or entities: Defendant
22 and Defendant's parents, subsidiaries, affiliates, officers, and directors, and any entity in which
23 Defendant has a controlling interest; all individuals who make a timely election to be excluded
24 from this proceeding using the correct protocol for opting out; and all judges assigned to hear any
25 aspect of this litigation, as well as their immediate family members.
26

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

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

3
4 200. Numerosity: Class Members are so numerous and geographically dispersed that
5 joinder of all members is impracticable. Upon information and belief, there likely millions of
6 individuals throughout the United States whose Personal and Financial Information has been
7 improperly used or disclosed by Defendant, and the Classes are identifiable within Defendant's
8 records.

9
10 201. Ascertainability. Class Members are readily identifiable from information in
11 Defendant's possession, custody, and control.

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

- 14 a. Whether Defendant disclosed Class Members' Personal and Financial Information to
15 Third Parties;
- 16 b. Whether Class Members consented to Defendant's disclosure of their Personal and
17 Financial Information;
- 18 c. Whether Defendant owed duties to Plaintiffs and Class Members to protect their
19 Personal and Financial Information;
- 20 d. Whether Defendant breached its duty to protect Plaintiffs' and Class Members'
21 Personal and Financial Information;
- 22 e. Whether Defendant's disclosure of Plaintiffs' and Class Members' Personal and
23 Financial Information to Third Parties violated federal, state and local laws, or industry
24 standards;
- 25
26
27
28

- 1 f. Whether Defendant's failure to allow Customers a meaningful opportunity to opt out
2 of sharing with Third Parties violated federal, state and local laws, or industry
3 standards;
- 4
- 5 g. Whether Defendant's conduct resulted in or was the actual cause of the disclosure of
6 Plaintiffs' and Class Members' and Personal and Financial Information;
- 7
- 8 h. Whether Defendant's conduct resulted in or was the proximate cause of the disclosure
9 of Plaintiffs' and Class Members' Personal and Financial Information;
- 10
- 11 i. Whether Defendant has a contractual obligation to protect Plaintiffs' and Class
12 Members' Personal and Financial Information and whether it complied with such
13 contractual obligation;
- 14
- 15 j. Whether Defendant has a duty sounding in bailment to protect Plaintiffs' and Class
16 Members' Personal and Financial Information and whether it complied with such
17 obligation;
- 18
- 19 k. Whether Defendant has a duty of confidence and whether it complied with such
20 obligation;
- 21
- 22 l. Whether Defendant's conduct amounted to violations of state consumer protection
23 statutes;
- 24
- 25 m. Whether Defendant's conduct amounted to violations of state and federal wiretap
26 statutes;
- 27
- 28 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;

1 p. Whether, as a result of Defendant's conduct, Plaintiffs and Class Members are entitled
2 to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such
3 relief.
4

5 203. Defendant has engaged in a common course of conduct toward Plaintiffs and the
6 Class Members, in that the Plaintiffs' and Class Members' data was stored on the same computer
7 system and unlawfully disclosed and accessed in the same way. As set forth above, the common
8 issues arising from Defendant's conduct affecting Class Members predominate over any
9 individualized issues. Adjudication of these common issues in a single action has important and
10 desirable advantages of judicial economy.
11

12 204. Typicality: Plaintiffs' claims are typical of those of other Class Members because
13 all had their Personal and Financial Information compromised as a result of Defendant's use and
14 incorporation of Facebook Pixel and other tracking technology.
15

16 205. Policies Generally Applicable to the Classes: This class action is also appropriate
17 for certification because Defendant has acted or refused to act on grounds generally applicable to
18 the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards
19 of conduct toward the Class Members and making final injunctive relief appropriate with respect
20 to the Classes as a whole. Defendant's policies challenged herein apply to and affect Class
21 Members uniformly, and Plaintiffs' challenge of these policies hinges on Defendant's conduct with
22 respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.
23

24 206. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests
25 of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be
26 antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or
27 adverse to the Class Members and the infringement of the rights and the damages Plaintiffs have
28

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

3
4 207. Superiority and Manageability: Class litigation is an appropriate method for fair
5 and efficient adjudication of the claims involved. Class action treatment is superior to all other
6 available methods for the fair and efficient adjudication of the controversy alleged herein; it will
7 permit a large number of Class Members to prosecute their common claims in a single forum
8 simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and
9 expense that hundreds of individual actions would require. Class action treatment will permit the
10 adjudication of relatively modest claims by certain Class Members, who could not individually
11 afford to litigate a complex claim against large corporations, like Defendant. Further, even for
12 those Class Members who could afford to litigate such a claim, it would still be economically
13 impractical and impose a burden on the courts.
14

15
16 208. The nature of this action and the nature of laws available to Plaintiffs and Class
17 Members make the use of the class action device a particularly efficient and appropriate procedure
18 to afford relief to Plaintiffs and Class Members for the wrongs alleged. If the class action device
19 were not used, Defendant would necessarily gain an unconscionable advantage because it would
20 be able to exploit and overwhelm the limited resources of each individual Class Member with
21 superior financial and legal resources. Moreover, the costs of individual suits could unreasonably
22 consume the amounts that would be recovered, whereas proof of a common course of conduct to
23 which Plaintiffs were exposed is representative of that experienced by the Classes and will
24 establish the right of each Class Member to recover on the cause of action alleged. Finally,
25 individual actions would create a risk of inconsistent results and would be unnecessary and
26 duplicative of this litigation.
27
28

1 209. The litigation of the claims brought herein is manageable. Defendant's uniform
2 conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class
3 Members demonstrates that there would be no significant manageability problems with
4 prosecuting this lawsuit as a class action.
5

6 210. Adequate notice can be given to Class Members directly using information
7 maintained in Defendant's records.
8

9 211. Unless a Class-wide injunction is issued, Defendant may continue in its unlawful
10 use and disclosure and failure to properly secure the Personal and Financial Information of
11 Plaintiffs and the Class Members, Defendant may continue to refuse to provide proper notification
12 to and obtain proper consent from Class Member, and Defendant may continue to act unlawfully
13 as set forth in this Complaint.
14

15 212. Moreover, Defendant has acted or refused to act on grounds generally applicable to
16 the Class, and, accordingly, final injunctive or corresponding declaratory relief regarding the whole
17 of the Classes is appropriate.
18

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

- 23 a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due
24 care in collecting, storing, using, and safeguarding their Personal and Financial
25 Information;
26
27
28

- 1 b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise
2 due care in collecting, storing, using, and safeguarding their Personal and Financial
3 Information;
- 4
- 5 c. Whether Defendant failed to comply with its own policies and applicable laws,
6 regulations, and industry standards relating to the disclosure of customer information;
- 7
- 8 d. Whether Defendant was negligent and/or negligent *per se*;
- 9
- 10 e. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs
11 and Class Members on the other, and the terms of that contract;
- 12
- 13 f. Whether Defendant breached the contract;
- 14
- 15 g. In the alternate, whether Defendant was unjustly enriched;
- 16
- 17 h. Whether a bailment existed between Defendant on the one hand, and Plaintiffs and
18 Class Members on the other;
- 19
- 20 i. Whether Defendant breached its bailment duty;
- 21
- 22 j. Whether Defendant adequately and accurately informed Plaintiffs and Class Members
23 that their Personal and Financial Information had been used and disclosed to Third
24 Parties and used for Third Party and fourth party benefit;
- 25
- 26 k. Whether Defendant adequately provided opt-out measures;
- 27
- 28 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,

1 p. Whether Plaintiffs and the Class Members are entitled to actual, consequential, and/or
2 nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.
3

4 **COUNT I**
5 **NEGLIGENCE**

6 **(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

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

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

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

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

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

24 219. Defendant acted with wanton and reckless disregard for the privacy and
25 confidentiality of Plaintiffs' and Class Members' Personal and Financial Information by disclosing
26
27
28

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

3
4 220. Defendant owed these duties to Plaintiffs and Class Members because they are
5 members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew
6 or should have known would suffer injury-in-fact from Defendant's disclosure of their Personal
7 and Financial Information to benefit Third Parties (and fourth parties) and Defendant. Defendant
8 actively sought and obtained Plaintiffs' and Class Members' Personal and Financial Information.
9 And Defendant knew or should have known that by integrating tracking technology on its Website
10 that Plaintiffs' and Class Members' nonpublic personal information, including Personal and
11 Financial Information, would be disclosed to the Third Parties (and used by the fourth parties).
12

13 221. Personal and Financial Information is highly valuable, and Defendant knew, or
14 should have known, the harm that would be inflicted on Plaintiffs and Class Members by disclosing
15 their Personal and Financial Information to the Third Parties. This disclosure was of benefit to the
16 Third Parties (and fourth parties) and Defendant by way of data harvesting, advertising, and
17 increased sales.
18

19 222. Defendant breached its duties by failing to exercise reasonable care in supervising
20 its agents, contractors, vendors, and suppliers in the handling and securing of Personal and
21 Financial Information of Plaintiffs and Class Members. This failure actually and proximately
22 caused Plaintiffs' and Class Members' injuries.
23

24 223. As a direct, proximate, and traceable result of Defendant's negligence and/or
25 negligent supervision, Plaintiffs and Class Members have suffered or imminently will suffer injury
26 and damages, including monetary damages, inappropriate advertisements and use of their Personal
27
28

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

3
4 224. Defendant's breach of its common-law duties to exercise reasonable care and
5 negligence, directly and proximately caused Plaintiffs' and Class Members' actual, tangible,
6 injury-in-fact and damages, including, without limitation: the unauthorized access of their Personal
7 and Financial Information by Third Parties (and fourth parties); improper disclosure of their
8 Personal and Financial Information; receipt of targeted advertisements reflecting private medical
9 information; lost benefit of their bargain; lost value of their Personal and Financial Information
10 and diminution in value; embarrassment, humiliation, frustration, and emotional distress; lost time
11 and money incurred to mitigate and remediate the effects of use of their information, as to targeted
12 advertisements that resulted from and were caused by Defendant's negligence; value to Plaintiffs
13 and the Class Members of surrendering their choices to keep their Personal and Financial
14 Information private and allowing Defendant to track their data; increased risk of future harm
15 resulting from future use and disclosure of Plaintiffs' and the Class Members' Personal and
16 Financial Information; and other injuries and damages as set forth herein. These injuries are
17 ongoing, imminent, immediate, and continuing.

18
19
20 225. Defendant's negligence directly and proximately caused the unauthorized access
21 and Disclosure of Plaintiffs' and Class Members' Personal and Financial Information, and as a
22 result, Plaintiffs and Class Members have suffered and will continue to suffer damages as a result
23 of Defendant's conduct. Plaintiffs and Class Members seek actual and compensatory damages, and
24 all other relief they may be entitled to as a proximate result of Defendant's negligence.

25
26 226. Plaintiffs and Class Members seek to recover the value of the unauthorized access
27 to their Personal and Financial Information resulting from Defendant's wrongful conduct. This
28

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

14
15
16
17 227. Plaintiffs and Class Members are also entitled to punitive damages resulting from
18 the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiffs
19 and Class Members in conscious disregard of their rights. Such damages are needed to deter
20 Defendant from engaging in such conduct in the future.

21
22 **COUNT II**
23 **NEGLIGENCE *PER SE***
24 **(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

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

26 229. Plaintiffs bring this negligence *per se* count in the alternative to their common law
27 negligence claim.
28

1 230. Pursuant to the laws set forth herein, including the FTC Act, the GLBA, and state
2 law, Defendant was required by law and industry standards to maintain adequate and reasonable
3 data and cybersecurity measures to maintain the security and privacy of Plaintiffs' and Class
4 Members' Personal and Financial Information.
5

6 231. Plaintiffs and Class Members are within the class of persons that these statutes and
7 rules were designed to protect.
8

9 232. Defendant had a duty to have procedures in place to detect and prevent the loss or
10 unauthorized dissemination of Plaintiffs' and Class Members' Personal and Financial Information.
11

12 233. Defendant owed a duty to timely and adequately inform Plaintiffs and Class
13 Members, in the event of their Personal and Financial Information being improperly disclosed to
14 unauthorized Third Parties.
15

16 234. It was not only reasonably foreseeable, but it was intended, that the failure to
17 reasonably protect and secure Plaintiffs' and Class Members' Personal and Financial Information
18 in compliance with applicable laws would result in unauthorized Third Parties gaining access to
19 Plaintiffs' and Class Members' Personal and Financial Information, and resulting in Defendant's
20 liability under principles of negligence *per se*.
21

22 235. Defendant violated its duty under Section 5 of the FTC Act, the GLBA, and/or state
23 law by failing to use reasonable measures to protect Plaintiffs' and Class Members' Personal and
24 Financial Information and not complying with applicable industry standards as described in detail
25 herein.
26

27 236. Plaintiffs' and Class Member's Personal and Financial Information constitutes
28 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.

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

3
4 243. Plaintiffs and Class Members communicated sensitive Personal and Financial
5 Information that they intended for only Defendant to receive and that they understood Defendant
6 would keep private.

7 244. Defendant's disclosure of the substance and nature of those communications to
8 Third Parties without the knowledge and consent of Plaintiffs and Class Members is an intentional
9 intrusion on Plaintiffs' and Class Members' solitude or seclusion in their private affairs and
10 concerns.
11

12 245. Plaintiffs and Class Members had a reasonable expectation of privacy given their
13 relationship with Defendant as a financial institution. Moreover, Plaintiffs and Class Members
14 have a general expectation that their communications regarding Personal and Financial
15 Information with their financial institution will be kept confidential. Defendant's disclosure of
16 Personal and Financial Information is highly offensive to the reasonable person.
17

18 246. As a result of Defendant's actions, Plaintiffs and Class Members have suffered
19 harm and injury, including but not limited to an invasion of their privacy rights under the California
20 Constitution.
21

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

25 248. Plaintiffs and Class Members seek appropriate relief for that injury, including but
26 not limited to, damages that will reasonably compensate Plaintiffs and Class Members for the harm
27 to their privacy interests as a result of its intrusions upon Plaintiffs' and Class Members' privacy.
28

1 255. By conduct complained of in the preceding paragraphs, Defendant violated Section
2 502(c)(1)(B) of CDAFA by knowingly accessing without permission Plaintiffs' and Class
3 Members' devices in order to wrongfully obtain and use their personal data, including their
4 Personal and Financial Information, in violation of Plaintiffs' and Class Members' reasonable
5 expectations of privacy in their devices and data.
6

7 256. Defendant violated Cal. Penal Code § 502(c)(2) by knowingly and without
8 permission accessing, taking, copying, and using Plaintiffs' and the Class Members' Personal and
9 Financial Information.
10

11 257. Defendant used Plaintiffs' and Class Members' data as part of a scheme to defraud
12 them and wrongfully obtain their data and other economic benefits. Specifically, Defendant
13 intentionally concealed from Plaintiffs and Class Members that Defendant had secretly installed
14 tracking pixels on its Online Platforms that surreptitiously shared Personal and Financial
15 Information with third party advertising companies like Facebook. Had Plaintiffs and Class
16 Members been aware of this practice, they would not have used Defendant's Website and Online
17 Platforms.
18

19 258. The computers and mobile devices that Plaintiffs and Class Members used when
20 accessing Defendant's Website all have and operate "computer services" within the meaning of
21 CDAFA. Defendant violated §§ 502(c)(of CDAFA by knowingly and without permission
22 accessing and using those devices and computer services, and/or causing them to be accessed and
23 used, *inter alia*, in connection with the Third Parties' (and fourth parties') wrongful use of such
24 data.
25

26 259. Under § 502(b)(12) of the CDAFA a "Computer contaminant" is defined as "any
27 set of computer instructions that are designed to . . . record, or transmit information within a
28

1 computer, computer system, or computer network without the intent or permission of the owner of
2 the information.”

3
4 260. Defendant violated § 502(c)(8) by knowingly and without permission introducing
5 a computer contaminant via trackers embedded into the Online Platforms which intercepted
6 Plaintiffs’ and the Class Members’ private and sensitive financial information.

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

- 9
10 a. Sensitive and confidential information that Plaintiffs and Class Members intended to
11 remain private is no longer private;
- 12 b. Defendant eroded the essential confidential nature of their relationship;
- 13 c. Defendant took something of value from Plaintiffs and Class Members and derived
14 benefit therefrom without Plaintiffs’ and Class Members’ knowledge or informed
15 consent and without sharing the benefit of such value;
- 16
17 d. Plaintiffs and Class Members did not get the full value of the financial services for
18 which they paid, which included Defendant’s duty to maintain confidentiality; and
- 19 e. Defendant’s actions diminished the value of Plaintiffs’ and Class Members’ Private
20 Information.

21
22 262. Plaintiffs and the Class Members seek compensatory damages in accordance with
23 Cal. Penal Code § 502(e)(1), in an amount to be proved at trial, and injunctive or other equitable
24 relief; as well as punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) as
25 Defendant’s violations were willful and, upon information and belief, Defendant is guilty of
26 oppression, fraud, or malice as defined in Cal. Civil Code § 3294; and reasonable attorney’s fees
27 under § 502(e)(2).
28

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

3
4 271. Plaintiffs and Class Members were reasonable to assume, and did assume, that
5 Defendant would take appropriate measures to keep their Personal and Financial Information
6 secure and not share it with Third Parties, or allow Third Parties (and fourth parties) to use
7 it, without their express consent. Defendant also had a duty to disclose that it was sharing their
8 Customers' Personal and Financial Information with Third Parties. However, Defendant did not
9 disclose at any time that it was sharing this Personal and Financial Information with Third Parties
10 via tracking technologies or that Third Parties (and fourth parties) were using their Personal and
11 Financial Information.

12
13 272. Had Plaintiffs and Class Members known that Defendant would intercept, collect,
14 and transmit their Personal and Financial Information to Third Parties, Plaintiffs and the Class
15 Members would not have used Defendant's services.

16
17 273. Plaintiffs and Class Members have a property interest in their Personal and
18 Financial Information. By surreptitiously collecting and otherwise misusing Plaintiffs' and Class
19 Members' Personal and Financial Information, Defendant has taken property from Plaintiffs and
20 Class Members without providing just (or indeed any) compensation.

21
22 274. By deceptively collecting, using, and sharing Plaintiffs' and Class Members'
23 Personal and Financial Information with Third Parties for Third Party (and fourth parties) use,
24 Defendant have taken money or property from Plaintiffs and Class Members. Accordingly,
25 Plaintiffs seek restitution on behalf of themselves and the Class.

26
27 275. Defendant's business acts and practices also meet the unfairness prong of
28 California's Unfair Competition Law ("UCL") according to all three theories of unfairness.

1 276. First, Defendant’s business acts and practices are “unfair” under the UCL pursuant
2 to the three-part test articulated in *Camacho v. Automobile Club of Southern California* (2006) 142
3 Cal. App. 4th 1394, 1403: (a) Plaintiffs and Class Members suffered substantial injury due to
4 Defendant’s Disclosure of their Personal and Financial Information; (b) Defendant’s disclosure of
5 Plaintiffs’ and Class Members’ Personal and Financial Information provides no benefit to
6 Customers, let alone any countervailing benefit that could justify Defendant’s Disclosure of
7 Personal and Financial Information without consent for marketing purposes or other pecuniary
8 gain; and (c) Plaintiffs and Class Members could not have readily avoided this injury because they
9 had no way of knowing that Defendant was implementing tracking technology.
10

11 277. Second, Defendant’s business acts and practices are “unfair” under the UCL
12 because they are “immoral, unethical, oppressive, unscrupulous, or substantially injurious” to
13 Plaintiffs and Class Members, and “the utility of [Defendant’s] conduct,” if any, does not
14 “outweigh the gravity of the harm” to Plaintiffs and Class Members. *Drum v. San Fernando Valley*
15 *Bar Ass’n*, (2010) 182 Cal. App. 4th 247, 257. Defendant secretly collected, disclosed, and
16 otherwise misused Plaintiffs’ and Class Members’ Personal and Financial Information by bartering
17 it to Third Parties in return for marketing and profit. This surreptitious, willful, and undisclosed
18 conduct is immoral, unethical, oppressive, unscrupulous, and substantially injurious. Moreover,
19 no benefit inheres in this conduct, the gravity of which is significant.
20

21 278. Third, Defendant’s business acts and practices are “unfair” under the UCL because
22 they run afoul of “specific constitutional, statutory, or regulatory provisions.” *Drum*, 182 Cal. App.
23 4th at 256 (internal quotation marks and citations omitted). California has a strong public policy
24 of protecting consumers’ privacy interests, including consumers’ personal data, as codified in
25 California’s Constitution in Article I, section 1; the California Invasion of Privacy Act, Cal. Penal
26
27
28

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

3
4 279. Defendant violated this public policy by, among other things, surreptitiously
5 collecting, disclosing, and otherwise exploiting Plaintiffs’ and Class Members’ Personal and
6 Financial Information by sharing that information with Third Parties via tracking technologies
7 without Plaintiffs’ and/or Class Members’ consent.

8
9 280. Had Plaintiffs and Class Members known Defendant would intercept, collect, and
10 transmit their Personal and Financial Information to Facebook and other Third Parties, Plaintiffs
11 and Class Members would not have used Defendant’s services.

12
13 281. Plaintiffs and Class Members were reasonable to assume, and did assume, that
14 Defendant would take appropriate measures to keep their Personal and Financial Information
15 secure and not share it with Third Parties without their express consent. Defendant was in sole
16 possession of and had a duty to disclose the material information that Plaintiffs’ and Class
17 Members’ Personal and Financial Information would be shared with Third Parties via trackers.
18 Defendant did not disclose at any time that they were sharing this Personal and Financial
19 Information with Third Parties via trackers.

20
21 282. Plaintiffs and Class Members have a property interest in their Personal and
22 Financial Information. By surreptitiously collecting and otherwise misusing Plaintiffs’ and Class
23 Members’ Personal and Financial Information, Defendant has taken property from Plaintiffs and
24 Class Members without providing just (or indeed any) compensation.

25
26 283. Plaintiffs and Class Members have lost money and property due to Defendant’s
27 conduct in violation of the UCL. Personal and Financial Information such as that which Defendant
28 collected and transmitted to Third Parties has objective monetary value. Companies are willing to

1 pay for Personal and Financial Information, like the information Defendant unlawfully collected
 2 and transmitted to Third Parties. For example, Pfizer annually pays approximately \$12 million to
 3 purchase similarly sensitive information on health data, from various sources.¹⁰⁸
 4

5 284. By deceptively collecting, using, and sharing Plaintiffs' and Class Members'
 6 Personal and Financial Information with Third Parties, and by allowing Third Parties (and fourth
 7 parties) to use their Personal and Financial Information, Defendant has taken money and/or
 8 property from Plaintiffs and Class Members. Accordingly, Plaintiffs seek restitution on behalf of
 9 themselves and the Class.
 10

11 285. As a direct and proximate result of Defendant's unfair and unlawful methods and
 12 practices of competition, Plaintiffs and Class Members suffered actual damages, including, but not
 13 limited to, the loss of the value of their Personal and Financial Information.
 14

15 286. As a direct and proximate result of its unfair and unlawful business practices,
 16 Defendant has each been unjustly enriched and should be required to make restitution to Plaintiffs
 17 and Class Members pursuant to §§ 17203 and 17204 of the California Business & Professions
 18 Code, disgorgement of all profits accruing to Defendant because of its unlawful and unfair business
 19 practices, declaratory relief, attorney fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5),
 20 and injunctive or other equitable relief.
 21

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

26 287. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.
 27

28 ¹⁰⁸ 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).

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

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

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

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

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

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

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

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

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

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

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

14
15
16
17 **COUNT VII**
18 **VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT,**
19 **CAL. CIV. CODE §§ 1798.80, *et seq.***
20 **(On Behalf of Plaintiffs and the California subclass)**

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

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

1 314. Plaintiffs and Class Members have an interest, both equitable and legal and
2 financial, in their Personal and Financial Information, that was conferred upon, collected by, and
3 maintained by Defendant and that was ultimately disclosed without their consent.
4

5 315. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the
6 form of valuable, sensitive, personal, and financial information—Personal and Financial
7 Information—that Defendant collected from Plaintiffs and Class Members under the guise of
8 keeping this information private. Defendant collected, used, and disclosed this information for its
9 own gain, for marketing purposes, and for sale or trade with Third Parties. Defendant did not share
10 this benefit with Plaintiffs and Class Members.
11

12 316. Plaintiffs and Class Members would not have used Defendant’s services, or would
13 have paid less for those services, if they had known that Defendant would collect, use, and disclose
14 their Personal and Financial Information to Third Parties or allow Third Parties (and fourth parties)
15 to use their Personal and Financial Information.
16

17 317. Defendant appreciated or had knowledge of the benefits conferred upon it by
18 Plaintiffs and Class Members.
19

20 318. The benefits that Defendant derived from Plaintiffs and Class Members rightly
21 belong to Plaintiffs and Class Members themselves. Under unjust enrichment principles, it would
22 be inequitable for Defendant to retain the profit and/or other benefits it derived from the unfair and
23 unconscionable methods, acts, and trade practices alleged in this Complaint.
24

25 319. Defendant continues to benefit and profit from its retention and use of Plaintiffs’
26 and Class Members’ Personal and Financial Information, while its value to Plaintiffs and Class
27 Members has been diminished.
28

1 further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here,
2 that are tortious and violate the terms of the federal and state statutes described in this complaint.
3

4 331. An actual controversy has arisen regarding Capital One's present and prospective
5 common law and other duties to keep its Customers' Personal and Financial Information
6 confidential and whether Defendant is currently keeping that information confidential. Plaintiffs
7 like Shah remain Capital One Customers who need to use the Capital One's Website to manage
8 accounts and the financial services provided them by Capital One. Plaintiffs Shah, Rose, and
9 similar Class Members thus remain at imminent risk that additional disclosure of their Personal
10 and Financial Information will occur in the future.
11

12 332. Pursuant to its authority under the Declaratory Judgment Act, this Court should
13 enter a judgment declaring, among other things, the following:
14

- 15 a. Defendant continues to owe a legal duty to secure Customers' Personal and Financial
16 Information, under the common law, Section 5 of the FTC Act, the GLBA, and various
17 state statutes;
- 18 b. Defendant continues to breach this legal duty by disclosing its Customers' Personal and
19 Financial Information, to unaffiliated Third Parties.
20

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

24 334. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable
25 injury, and lack an adequate legal remedy. The risk of additional disclosure is real, immediate, and
26 substantial, as trackers remain operative on Defendant's website to this day. If additional disclosure
27 occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of
28

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

3
4 335. The hardship to Plaintiffs and Class Members if an injunction does not issue
5 exceeds the hardship to Defendant if an injunction is issued. Among other things, if Capital One
6 continues to disclose its Customers' Personal and Financial Information, Plaintiffs and Class
7 Members will likely be subjected to the harms described herein. On the other hand, the cost to
8 Defendant of complying with an injunction by keeping its Customers' Personal and Financial
9 Information, confidential is relatively minimal (for example, removing trackers from its website),
10 and Defendant has a pre-existing legal obligation to do so.

11
12 336. Issuance of the requested injunction will not disserve the public interest. To the
13 contrary, such an injunction would benefit the public by preventing Capital One's additional
14 unlawful disclosures of Customers' Personal and Financial Information, thus eliminating the
15 additional injuries that would result to Plaintiffs and the hundreds of thousands of Customers
16 whose information has been and will continue to be disclosed.

17
18 **COUNT XII**
19 **BREACH OF CONFIDENCE**
20 **(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

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

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

25 339. As alleged herein and above, Capital One's relationship with Plaintiffs and Class
26 Members was governed by terms and expectations that Plaintiffs' and Class Members' Personal
27 and Financial Information, would be collected, stored, and protected in confidence, and would not
28

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

3
4 340. Plaintiffs and Class Members provided Capital One with their Personal and
5 Financial Information, with the explicit and implicit understandings that Capital One would protect
6 and not permit that information to be disseminated to and used by unaffiliated Third Parties (and
7 fourth parties) without notice, consent, and sufficient opportunity to opt out.

8
9 341. Capital One voluntarily received in confidence Plaintiffs' and Class Members'
10 Personal and Financial Information, with the understanding and affirmative representation to
11 Customers that the information would not be disclosed or disseminated to unaffiliated Third Parties
12 for Third Parties' (and fourth parties') marketing purposes.

13
14 342. Capital One disclosed Plaintiffs' and Class Members' Personal and Financial
15 Information, without notice, without express permission, and without opportunity to opt out.

16
17 343. But for Capital One's Disclosure of Plaintiffs' and Class Members' Personal and
18 Financial Information, in violation of the parties' understanding of confidence, their Personal and
19 Financial Information would not have been disclosed to Third Parties, or used for Third Party (and
20 fourth party) marketing and profit, without their consent.

21
22 344. The injury and harm Plaintiffs and Class Members suffered was the reasonably
23 foreseeable result of Capital One's nonconsensual disclosure of Plaintiffs' and Class Members'
24 Personal and Financial Information. Capital One knew it was disclosing Plaintiffs' and Class
25 Members' Personal and Financial Information to Third Parties, for Third Party (and fourth party)
26 use, without their consent.
27
28

1 345. As a direct and proximate result of Capital One’s breaches of confidence, Plaintiffs
2 and Class Members have been injured and are entitled to damages in an amount to be proven at
3 trial.
4

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

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

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

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

13 ...advances in science and technology have led to the development of new devices
14 and techniques for the purpose of eavesdropping upon private communications and
15 that the invasion of privacy resulting from the continual and increasing use of such
16 devices and techniques has created a serious threat to the free exercise of personal
17 liberties and cannot be tolerated in a free and civilized society.

18 The Legislature by this chapter intends to protect the right of privacy of the people
19 of this state.

20 Cal. Penal Code §§ 630.

21 349. Cal. Penal Code § 631(a) prohibits persons from “aid[ing], agree[ing] with,
22 employ[ing], or conspir[ing] with” a third party to “read[], or attempt[] to read, or to learn the
23 contents or meaning of any message, report, or communication while the same is in transit or
24 passing over any wire, line, or cable, or is being sent from, or received at any place within this
25 state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any
26 way, any information so obtained” “by means of any machine, instrument, or contrivance, or in
27 any other manner...” Cal. Penal Code § 631(a).
28

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

3
4 351. All alleged communications between individual Plaintiffs or Class Members and
5 Defendant qualify as protected communications under CIPA because each communication is made
6 using personal computing devices (e.g., computers, smartphones, tablets) that send and receive
7 communications in whole or in part through the use of facilities used for the transmission of
8 communications aided by wire, cable, or other like connections.

9
10 352. As alleged in the preceding paragraphs, by use of the tracking technology,
11 Defendant used a recording device to record the confidential communications including Personal
12 and Financial Information without the consent of Plaintiffs or Class Members and then transmitted
13 such information to Third Parties for Third Party (and fourth party) use.

14
15 353. At all relevant times, Defendant's aiding of Third Parties to learn the contents of
16 communications and Defendant's recording of confidential communications was without
17 Plaintiffs' and the Class Members' authorization and consent.

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

23
24 355. Defendant engaged in and continued to engage in interception by aiding others
25 (including Facebook) to secretly record the contents of Plaintiffs' and Class Members' wire
26 communications.

27
28 356. The intercepting devices used in this case include, but are not limited to:

- 1 a. Those to which Plaintiffs' and Class Members' communications were disclosed;
- 2 b. Plaintiffs' and Class Members' personal computing devices;
- 3 c. Plaintiffs' and Class Members' web browsers;
- 4 d. Plaintiffs' and Class Members' browser-managed files;
- 5 e. Trackers like the Meta Pixel;
- 6 f. Internet cookies;
- 7 g. Other pixels, trackers, and/or tracking technology installed on Defendant's Website
- 8 and/or server;
- 9 h. Defendant's computer servers;
- 10 i. Third Party source code utilized by Defendant; and
- 11 j. Third Party computer servers (including Facebook).

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

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

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

1 360. The trackers that Defendant utilized are designed such that they transmitted each of
2 a website user's actions to Third Parties alongside and contemporaneously with the user initiating
3 the communication. Thus, Plaintiffs and Class Members' communications were intercepted in
4 transit to the intended recipient (Defendant) before they reached Defendant's servers.
5

6 361. Defendant willingly facilitated the Third Parties' interception and collection of
7 Plaintiffs' and Class Members' Personal and Financial Information, and the Third Parties' (and
8 fourth parties') use of their Personal and Financial Information, by embedding trackers on its
9 Website. Moreover, Defendant had full control over these trackers, including which webpages
10 contained the pixels, what information was tracked and shared, and how events were categorized
11 prior to transmission.
12

13 362. Defendant gave substantial assistance to Third Parties in violating the privacy rights
14 of Capital One's Customers, even though Defendant's conduct constituted a breach of the
15 confidentiality duties that it owed, including the duty financial institutions owe to their customers
16 and customers' property. Defendant knew that the installation of trackers on its website would
17 result in the unauthorized disclosure of its Customers' communications to Third Parties, and Third
18 Party (and fourth party) use of those communications, yet nevertheless did so anyway.
19

20 363. Plaintiffs' and Class Members' electronic communications were intercepted during
21 transmission, without their consent, for the unlawful and/or wrongful purpose of monetizing their
22 Personal and Financial Information, including using their Personal and Financial Information to
23 develop marketing and advertising strategies.
24

25 364. The Personal and Financial Information that Defendant assisted Third Parties with
26 reading, learning, and exploiting, included Plaintiffs' and Class Members' Personal and Financial
27 Information customers input into and accessed on Capital One's Website. Capital One disclosed
28

1 details about Customers, like Plaintiffs and Class Personal and Financial Information and their
2 interactions with Capital One’s website as users applied for credit cards, including the fact that a
3 user was on a certain page, that users clicked buttons and what URLs or webpages they led to,
4 information entered on preapproval application pages including employment, bank accounts, and
5 Customers’ eligibility, pre-approval, or approval for a credit card.
6

7 365. Plaintiffs and the Class Members seek statutory damages under Cal. Penal Code §
8 637.2(a), which provides for the greater of: (1) \$5,000 per violation; or (2) three times the amount
9 of damages sustained by Plaintiffs and the Classes in an amount to be proven at trial, as well as
10 injunctive or other equitable relief.
11

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

- 14 a. Sensitive and confidential information that Plaintiffs and Class Members intended to
15 remain private is no longer private.
- 16 b. Defendant eroded the essential confidential nature of the banker-customer, and specifically
17 the creditor-debtor, relationship.
- 18 c. Defendant took something of value from Plaintiffs and Class Members and derived benefit
19 therefrom without Plaintiffs’ and Class Members’ knowledge or informed consent and
20 without sharing the benefit of such value;
- 21 d. Plaintiffs and Class Members did not get the full value of the financial services for which
22 they paid, which included Defendant’s duty to maintain confidentiality; and
- 23 e. Defendant’s actions diminished the value of Plaintiffs’ and Class Members’ Personal and
24 Financial Information.
25
26
27
28

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

3
4 **COUNT XIV**
5 **VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (“ECPA”)**
6 **18 U.S.C. §§ 2511(1), et seq.**
7 **(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

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

9 369. The ECPA protects both sending and receipt of communications. 18 U.S.C. §
10 2520(a) provides a private right of action to any person whose wire or electronic communications
11 are intercepted, disclosed, or intentionally used in violation of Chapter 119.

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

15 371. **Electronic Communications.** The transmission of Personal and Financial
16 Information between Plaintiffs and Class Members and Defendant’s Website with which they
17 chose to exchange communications are “transfer[s] of signs, signals, writing,...data, [and]
18 intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic,
19 photoelectronic, or photo optical system that affects interstate commerce” and are therefore
20 “electronic communications” within the meaning of 18 U.S.C. § 2510(2).

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

24 373. **Interception.** The ECPA defines the interception as the “acquisition of the contents
25 of any wire, electronic, or oral communication through the use of any electronic, mechanical, or
26
27
28

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

3
4 374. **Electronic, Mechanical or Other Device.** The ECPA defines “electronic,
5 mechanical, or other device” as “any device...which can be used to intercept a[n]...electronic
6 communication[.]” 18 U.S.C. § 2510(5). The following constitute “devices” within the meaning
7 of 18 U.S.C. § 2510(5):

- 8 a. Plaintiffs’ and Class Members’ browsers;
9
10 b. Plaintiffs’ and Class Members’ computing devices;
11
12 c. Defendant’s web-servers;
13
14 d. Defendant’s Website; and
15
16 e. The tracking technology deployed by Defendant effectuated the sending and acquisition of
17 customer communications.

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

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

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

27 378. By intentionally disclosing or endeavoring to disclose the electronic
28 communications of Plaintiffs and Class Members to Third Parties, while knowing or having reason

1 to know that the information was obtained through the interception of an electronic communication
2 in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

3
4 379. By intentionally using, or endeavoring to use, the contents of the electronic
5 communications of Plaintiffs and Class Members, while knowing or having reason to know that
6 the information was obtained through the interception of an electronic communication in violation
7 of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

8
9 380. **Unauthorized Purpose.** Defendant intentionally intercepted the contents of
10 Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious
11 act in violation of the Constitution or laws of the United States or of any State – namely, invasion
12 of privacy, among others.

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

15
16 382. Defendant specifically used tracking technology to track and to utilize Plaintiffs'
17 and Class Members' Personal and Financial Information for financial gain.

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

20
21 384. Plaintiffs and Class Members did not authorize Defendant to acquire the content of
22 their communications for purposes of invading Plaintiffs' and Class Members' privacy via the
23 tracking technology.

24 385. In sending and in acquiring the content of Plaintiffs' and Class Members'
25 communications relating to the browsing of its Website, Defendant's purpose was tortious,
26 criminal and designed to violate federal and state legal provisions, including as described above
27 the following: (i) a knowing intrusion into a private, place, conversation or matter that would be
28

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

3
4 **COUNT XV**
5 **VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT**
6 **18 U.S.C. § 2511(3)(a)**
7 **UNAUTHORIZED DIVULGENCE BY ELECTRONIC COMMUNICATIONS SERVICE**
8 **(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

9
10 386. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

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

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

23 389. **Intentional Divulgence.** Defendant intentionally designed the tracking technology
24 and was or should have been aware that, if so configured, it could divulge Plaintiffs’ and Class
25 Members’ Personal and Financial Information. Upon information and belief, Defendant’s
26 divulgence of the contents of Plaintiffs’ and Class Members’ communications was
27
28

1 contemporaneous with their exchange with Defendant’s Website, to which they directed their
2 communications.

3
4 390. Defendant divulged the contents of Plaintiffs’ and Class Members’ electronic
5 communications without authorization and/or consent.

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

8
9 “[a] person or entity providing electronic communication service to the public may
10 divulge the contents of any such communication”...“as otherwise authorized in
11 section 2511(2)(a) or 2517 of this title; “with the lawful consent of the originator
12 or any addressee or intended recipient of such communication;” c. “to a person
13 employed or authorized, or whose facilities are used, to forward such
14 communication to its destination;” or d. “which were inadvertently obtained by the
15 service provider and which appear to pertain to the commission of a crime, if such
16 divulgence is made to a law enforcement agency.”

17 U.S.C. § 2511(3)(b).

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

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

28 ¹⁰⁹ 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).

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

3
4 394. Section 2517 of the ECPA relates to investigations by government officials and has
5 no relevance here.

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

12
13 396. Moreover, Defendant divulged the contents of Plaintiffs’ and Class Members’
14 communications through tracking technology to individuals who are not “person[s] employed or
15 whose facilities are used to forward such communication to its destination.”

16
17 397. The contents of Plaintiffs’ and Class Members’ communications did not appear to
18 pertain to the commission of a crime and Defendant did not divulge the contents of their
19 communications to a law enforcement agency.

20
21 398. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may
22 assess statutory damages, preliminary and other equitable or declaratory relief as may be
23 appropriate, punitive damages in an amount to be determined by a jury and a reasonable attorney’s
24 fee and other litigation costs reasonably incurred.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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.

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

3
4 “may divulge the contents of a communication—” a. “to an addressee or intended
5 recipient of such communication or an agent of such addressee or intended
6 recipient.” b. “as otherwise authorized in Section 2517, 2511(2)(a), or 2703 of this
7 title;” c. “with the lawful consent of the originator or an addressee or intended
8 recipient of such communication, or the subscriber in the case of remote computing
9 service;” d. “to a person employed or authorized or whose facilities are used to
10 forward such communication to its destination;” e. “as may be necessarily incident
11 to the rendition of the service or to the protection of the rights or property of the
12 provider of that service;” f. “to the National Center for Missing and Exploited
13 Children, in connection with a reported submission thereto under section 2258A.”
14 g. “to a law enforcement agency, if the contents (i) were inadvertently obtained by
15 the service provider; and (ii) appear to pertain to the commission of a crime;” h. “to
16 a governmental entity, if the provider, in good faith, believes that an emergency
17 involving danger of death or serious physical injury to any person requires
18 disclosure without delay of communications relating to the emergency”; or “to a
19 foreign government pursuant to an order from a foreign government that is subject
20 to an executive agreement that the Attorney General has determined and certified
21 to Congress satisfies Section 2523.”

22 407. Defendant did not divulge the contents of Plaintiffs’ and Class Members’
23 communications to “addressees,” “intended recipients,” or “agents” of any such addressees or
24 intended recipients of Plaintiffs and Class Members.

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

27 409. Section 2511(2)(a)(i) provides: It shall not be unlawful under this chapter for an
28 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

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

3
4 410. Defendant's divulgence of the contents of Plaintiffs' and Class Members'
5 communications on its Website to Third Parties was not authorized by 18 U.S.C. § 2511(2)(a)(i)
6 in that it was neither: (i) a necessary incident to the rendition of the Defendant's services nor (ii)
7 necessary to the protection of the rights or property of Defendant.

8
9 411. Section 2517 of the ECPA relates to investigations by government officials and has
10 no relevance here.

11
12 412. Defendant's divulgence of the contents of Plaintiffs' and Class Members' customer
13 user communications on its Website was not done "with the lawful consent of the originator or any
14 addresses or intended recipient of such communication[s]." As alleged above: (i) Plaintiffs and
15 Class Members did not authorize Defendant to divulge the contents of their communications and
16 (ii) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiffs
17 and Class Members were exchanging information.

18
19 413. Moreover, Defendant divulged the contents of Plaintiffs' and Class Members'
20 communications through the tracking technology to individuals who are not "person[s] employed
21 or whose facilities are used to forward such communication to its destination."

22
23 414. The contents of Plaintiffs' and Class Members' communications did not appear to
24 pertain to the commission of a crime and Defendant did not divulge the contents of their
25 communications to a law enforcement agency.

26
27 415. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may
28 assess statutory damages, preliminary and other equitable or declaratory relief as may be

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

3
4 **COUNT XVII**
5 **VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT ("CFAA")**
6 **18 U.S.C. §§ 1030, et seq.**
7 **(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

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

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

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

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

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

23 421. Accordingly, Plaintiffs and the Class Members are entitled to "maintain a civil
24 action against the violator to obtain compensatory damages and injunctive relief or other equitable
25 relief." 18 U.S.C. § 1030(g).
26
27
28

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;

- 1 I. Costs and any other expenses, including expert witness fees incurred by Plaintiffs
2 in connection with this action;
3
4 J. Pre- and post-judgment interest on any amounts awarded; and
5
6 K. Such other and further relief as this court may deem just and proper.

6 **JURY DEMAND**

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

9 Dated: August 26, 2024

10 Respectfully submitted,

11 

12
13 Natalie Lyons, No. 293026
14 Vess A. Miller, No. 278020
15 Lynn A. Toops*
16 Amina A. Thomas*
17 COHEN & MALAD, LLP
18 One Indiana Square, Suite 1400
19 Indianapolis, Indiana 46204
20 (317) 636-6481
nlyons@cohenandmalad.com
vmiller@cohenandmalad.com
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

21 J. Gerard Stranch, IV*
22 Emily E. Schiller*
23 STRANCH, JENNINGS & GARVEY, PLLC
24 223 Rosa L. Parks Avenue, Suite 200
25 Nashville, Tennessee 37203
26 (615) 254-8801
27 (615) 255-5419 (facsimile)
gstranch@stranchlaw.com
eschiller@stranchlaw.com

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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***

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Capital One Illegally Shared Website Visitors' Private Info with Third Parties, Class Action Lawsuit Says](#)
