

1 HERRERA PURDY LLP
Shawn M. Kennedy (SBN 218472)
2 *skennedy@herrerapurdy.com*
Andrew M. Purdy (SBN 261912)
3 *apurdy@herrerapurdy.com*
Bret D. Hembd (SBN 272826)
4 *bhembd@herrerapurdy.com*
4590 MacArthur Blvd., Suite 500
5 Newport Beach, CA 92660
Tel: (949) 936-0900
6 Fax: (855) 969-2050

LIEFF CABRASER HEIMANN &
BERNSTEIN, LLP
Michael W. Sobol (SBN 194857)
msobol@lchb.com
Melissa Gardner (SBN 289096)
mgardner@lchb.com
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Tel: (415) 956-1000
Fax: (415) 956-1008

7 HERRERA PURDY LLP
Nicomedes Sy Herrera (SBN 275332)
8 *nherrera@herrerapurdy.com*
Laura E. Seidl (SBN 269891)
9 *lseidl@herrerapurdy.com*
1300 Clay Street, Suite 600
10 Oakland, CA 94612
Tel: (510) 422-4700
11 Fax: (855) 969-2050

BURNS CHAREST LLP
Warren T. Burns (*Pro Hac Vice* to be Filed)
wburns@burnscharest.com
Russell Herman (*Pro Hac Vice* to be Filed)
rherman@burnscharest.com
900 Jackson Street, Suite 500
Dallas, TX 75202
Tel: (469) 904-4550
Fax: (469) 444-5002

12 LIEFF CABRASER HEIMANN &
BERNSTEIN, LLP
13 Rachel Geman (*Pro Hac Vice* to be Filed)
rgeman@lchb.com
14 250 Hudson Street, 8th Floor
New York, NY 10013-1413
15 Tel: (212) 355-9500
16 Fax: (212) 355-9592

BURNS CHAREST LLP
Christopher J. Cormier
(*Pro Hac Vice* to be Filed)
ccormier@burnscharest.com
5290 Denver Tech Center Parkway, Suite 150
Greenwood Village, CO 80111
Tel: (720) 630-2092
Fax: (469) 444-5002

17 *Attorneys for Plaintiffs and the Proposed Classes*

18 [Additional counsel on signature page]

19 UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
20 SAN FRANCISCO DIVISION

21 JAMES COTTLE and FREDERICK
SCHOENEMAN, on behalf of
22 themselves and all others similarly
23 situated,

24 Plaintiffs,

25 v.

26 PLAID INC., a Delaware corporation,

27 Defendant.
28

Case No.: _____

**COMPLAINT FOR DAMAGES AND
DECLARATORY AND EQUITABLE
RELIEF**

CLASS ACTION

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

1			
2			<u>Page</u>
3	I.	INTRODUCTION	1
4	II.	JURISDICTION AND VENUE	2
5	III.	INTRADISTRICT ASSIGNMENT	3
6	IV.	THE PARTIES	3
7	V.	FACTUAL BACKGROUND.....	4
8		A. Background of Plaid and the Participating Apps.....	4
9		B. Plaid Deceptively Obtains Bank Account Credentials from App Users	6
10		C. Plaid Leverages Credentials to Collect Valuable Data on a Massive Scale	12
11		D. Plaid Sells and Otherwise Exploits the Unlawfully-Obtained Private Data.....	16
12		E. Plaid and Its Fintech Clients Conceal Plaid’s Conduct from Consumers	18
13		F. Plaid’s Harm to Consumers is Recognized by Banks and Industry Groups.....	25
14		G. Plaid Knowingly Violates Established Industry Standards and Obligations.....	29
15		1. The GLBA Standards	29
16		2. Plaid’s Acknowledgement of Its Disclosure Obligations.....	31
17		3. Violations of GLBA Standards in Plaid’s Privacy Policy	33
18	VI.	INJURY AND DAMAGES TO THE CLASS	35
19		A. The Named Plaintiffs’ Experiences	35
20		B. Injuries from Invasions of Privacy and Dignitary Violations.....	39
21		C. Economic Damages	42
22		1. Loss of Valuable Indemnification Rights	42
23		2. Diminished Value of Rights to Protection of Data.....	45
24		3. Loss of Control Over Property with Marketable Value.....	45
25		4. Increased Risk of Identity Theft and Fraud	46
26	VII.	CHOICE OF LAW	47
27	VIII.	TOLLING, CONCEALMENT, AND ESTOPPEL.....	47
28	IX.	CLASS ACTION ALLEGATIONS	48
	X.	CLAIMS FOR RELIEF	53
		PRAYER FOR RELIEF	80
		DEMAND FOR JURY TRIAL	82

1 Plaintiffs James Cottle and Frederick Schoeneman (“Plaintiffs”), individually and as
2 representatives of a class of similarly situated persons, by their undersigned counsel, allege as
3 follows against Defendant Plaid Inc. (“Plaid”):

4 **I. INTRODUCTION**

5 1. Among the most valuable and sensitive of all consumer data is the personal
6 financial information maintained in consumers’ banking and other financial accounts. The
7 common law of privacy, as well as many federal and state laws, safeguard such information.
8 Contrary to these laws and societal norms, Plaid takes consumers’ financial account login
9 credentials, accesses their banking and other financial accounts several times per day, and then
10 sells and otherwise misuses the highly personal and private information it has wrongfully
11 obtained. Plaid discloses none of this to consumers.

12 2. Plaid gathers all this data through software embedded in widely-used financial
13 technology (fintech) apps such as Venmo, Coinbase, Square’s “Cash App,” and Stripe. Plaid’s
14 stated mission is to make it “easy” for consumers to “connect” their bank accounts to these
15 fintech apps, but Plaid conceals its conduct and true intentions from consumers. Indeed, Plaid for
16 years has exploited its position as middleman to acquire app users’ banking login credentials and
17 then use those credentials to harvest vast amounts of private transaction history and other
18 financial data, all without consent. Plaid has perpetrated this scheme to amass what it touts as
19 “one of the largest transactional data sets in the world.”

20 3. First, Plaid induces consumers to hand over their private bank login credentials to
21 *Plaid* by making it appear those credentials are being communicated directly to consumers’
22 *banks*. Consumers are informed the connection is “private” and “secure,” and their banking
23 credentials will “never be made accessible” to the app. They are then directed to a login screen
24 that looks like it is coming from their bank, complete with the bank’s logo and branding. In
25 reality, however, though Plaid does not disclose this, the login screen is created by, controlled by,
26 and connected to Plaid. Plaid executives have acknowledged this process was “optimized” to
27 increase “user conversions”—in other words, to provide a false sense of comfort to consumers by
28 concealing Plaid’s role as an unaffiliated third party.

1 4. Second, Plaid uses consumers' login credentials to obtain *direct and full* access to
2 consumers' personal financial banking information for Plaid's own commercial purposes wholly
3 unrelated to consumers' use of the apps. For each consumer, Plaid downloads years' worth of
4 transaction history for *every single account* they have connected to that bank (such as checking,
5 savings, credit card, and brokerage accounts), regardless of whether the data in any of the
6 accounts bears any relationship to the app for which the consumer signed up. Thus, a consumer
7 who makes a single mobile payment on an app from a checking account unwittingly gives Plaid
8 years' worth of private, granular financial information from every account the consumer
9 maintains with the bank, including accounts maintained for others such as relatives and children.
10 To date, Plaid has amassed this trove of data from over **200 million** distinct financial accounts.

11 5. Plaid exploits its ill-gotten information in a variety of ways, including marketing
12 the data to its app customers, analyzing the data to derive insights into consumer behavior, and,
13 most recently, selling its collection of data to Visa as part of a multi-billion dollar acquisition.
14 Plaid has unfairly benefited from the personal information of millions of Americans and
15 wrongfully intruded upon their private financial affairs.

16 6. Accordingly, Plaintiffs, on behalf of themselves and similarly-situated consumers,
17 bring this action to seek declaratory and injunctive relief requiring Plaid to cease its misconduct,
18 purge the data it has unlawfully collected, notify consumers of its misconduct, and inform
19 consumers of the steps they can take to protect themselves from further invasions. Plaintiffs also
20 seek economic redress for Plaid's violations of consumers' dignitary rights, privacy, and well-
21 being caused by Plaid's unethical and undisclosed invasions into their financial affairs.

22 **II. JURISDICTION AND VENUE**

23 7. Pursuant to 28 U.S.C. § 1331, this Court has original subject matter jurisdiction
24 over the claims that arise under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and the
25 Stored Communications Act, 18 U.S.C. § 2701.

26 8. This Court also has supplemental jurisdiction over the asserted state law claims
27 pursuant to 28 U.S.C. § 1367.
28

1 9. This Court has diversity jurisdiction pursuant to 28 U.S.C. § 1332(d) under the
2 Class Action Fairness Act because the amount in controversy exceeds \$5,000,000, exclusive of
3 interest and costs, and at least one Class member is a citizen of a state different from Plaid.

4 10. This Court has personal jurisdiction over Defendant because Plaid has conducted
5 business in the State of California, and because Plaid has committed acts and omissions
6 complained of herein in the State of California.

7 11. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Plaid does
8 business in and is subject to personal jurisdiction in this District. Venue is also proper because a
9 substantial part of the events or omissions giving rise to the claims occurred in or emanated from
10 this District.

11 **III. INTRADISTRICT ASSIGNMENT**

12 12. Pursuant to Civil L.R. 3-2(c), assignment to the San Francisco Division of this
13 District is proper because a substantial part of the conduct which gives rise to Plaintiffs' claims
14 occurred in the City and County of San Francisco. Plaid markets and deploys its products
15 throughout the United States, including in San Francisco. Additionally, Plaid is headquartered in
16 San Francisco and developed the software at issue in this action in this District.

17 **IV. THE PARTIES**

18 13. **Plaintiff James Cottle** is a citizen and resident of the State of California.

19 14. **Plaintiff Frederick Schoeneman** is a citizen and resident of the State of
20 California.

21 15. **Defendant Plaid Inc.** is a financial technology company that describes its
22 business as building the technical infrastructure that connects consumers, financial institutions,
23 and fintech developers. In addition, Plaid says that it delivers “key insights” on top of data access
24 through its suite of analytics products.¹ Plaid is a Delaware corporation with its principal place of
25 business at 85 Second Street, Suite 400, San Francisco, California 94105.

26
27
28

¹ See <https://plaid.com/company/>.

1 **V. FACTUAL BACKGROUND**

2 **A. Background of Plaid and the Participating Apps**

3 16. Plaid was founded in 2012 by Zach Perret and William Hockey. The two initially
4 founded Plaid with the intention of building a consumer-facing fintech app. By early 2013,
5 however, they pivoted to building a behind-the-scenes data aggregator and data brokerage
6 operation: the fintech infrastructure product known as Plaid.²

7 17. Although Plaid's co-founders conceal Plaid's true nature and intentions from
8 consumers, they evidenced their actual intentions within the financial technology industry early in
9 the company's existence while they were still formulating their strategy. As early as February
10 2013, when Perret and Hockey introduced Plaid at the insular "NYC Data Business Meetup," the
11 co-founders made clear that Plaid's true purpose is to monetize consumer transactional and other
12 banking data. Collecting and aggregating data from financial institutions was merely the "table
13 stakes," as Plaid's real goal was to "resolve data and make that something interesting." They
14 emphasized the "immense" amount of consumer spending data the company could collect from
15 banks—going back up to five years—and the "awesome" things Plaid could do with the data. At
16 that time, they reported that Plaid could collect detailed information regarding 3,700 transactions
17 (covering about \$190,000 of spending) for the average consumer, along with 1,750 unique
18 geolocations to which the transactions were mapped. Perret explained that this broad and
19 extensive data collection sets Plaid apart from other apps in the "tried and true" bank-connection
20 and data-aggregation process.³

21 18. Further, in a February 2013 thread on Y Combinator's Hacker News forum,
22 Hockey stated that Plaid's software made it simple for an application to link with consumer credit
23 and debit card spending data—a convenience that would eventually rocket Plaid into use by more
24 than 2,000 applications today. Hockey also stated (but would keep hidden from consumers) that
25

26 ² See Apr. 13, 2018 Forbes Article: *Fintech's Happy Plumbers*, <https://www.forbes.com/plaid-fintech/#3c71271167f9>; 5/13/19 interview with Zach Perret at Data Driven NYC event, <https://www.youtube.com/watch?v=sgnCs34mopw>.

27
28 ³ See Feb. 2013 presentation by Zach Perret and William Hockey at NYC Data Business Meetup at 2:28 to 7:52, https://www.youtube.com/watch?v=_I8DRbFmLKM.

1 in the process of providing that connection, Plaid was “generating one of the largest transactional
2 data sets in the world, and using machine learning and statistical analysis to draw insights about
3 how consumers spend their time, money, and attention.”⁴ Similarly, in a different thread on the
4 same forum a month later, Perret stated that Plaid was “building the missing API [Application
5 Programming Interface]⁵ for Spending Data,” and that in the process, Plaid was “generating one
6 of the largest transactional data sets in the world, and using machine learning to draw insights
7 about how consumers spend their time, money, and attention.”⁶

8 19. Even Plaid’s company name is a hidden tribute to its true purpose (contrary to its
9 public image as an infrastructure tool, to the extent the public learns of Plaid at all), which is
10 monetizing consumer transactional data. According to co-founder Perret, he and Hockey came up
11 with the name “Plaid” based on the cross-hatch patterns formed when they mapped out how their
12 algorithm worked to compare consumers’ spending patterns with those of other consumers, while
13 also matching those consumers’ transaction data to Plaid’s nationwide merchant database.⁷

14 20. Not surprisingly, as fintech developers became aware of the scale and depth of
15 data Plaid could deliver, they also recognized its value to their own businesses.⁸ One of the
16 earliest such developers was Venmo, whose head of development approached Plaid about
17 incorporating its software.⁹ At that time, the main focus of Plaid’s software was the delivery of
18 extensive transaction data for the purpose of running analytics on the data.

19
20
21 ⁴ See <https://news.ycombinator.com/item?id=5216710>.

22 ⁵ See <https://news.ycombinator.com/item?id=5304169>. An Application Programming Interface is
a software intermediary that allows two applications to communicate with each other.

23 ⁶ See <https://news.ycombinator.com/item?id=5304169>.

24 ⁷ See May 13, 2019 interview with Zach Perret at Data Driven NYC event at 10:45 to 11:45,
<https://www.youtube.com/watch?v=sgnCs34mopw>.

25 ⁸ See *Plaid Launches the “Modern API for Banking Data,”*
<https://homebrew.co/blog/2013/09/19/plaid-launches-the-modern-api-for-banking-data>
26 (“Everyone said ‘Yes, but where do we get that data? We’d absolutely love to use it.’ So Zach
and William decided to turn Plaid from an app into an API.”).

27 ⁹ See May 13, 2019 interview with Zach Perret at Data Driven NYC event at 19:44 to 19:51,
<https://www.youtube.com/watch?v=sgnCs34mopw>. At the time, Venmo was an independent
28 corporate entity registered in New York (Venmo LLC). In 2015, Venmo was acquired by PayPal,
Inc. and subsequently merged with that corporation.

1 21. During the following years, Plaid succeeded in getting its software embedded in a
2 vast array of popular consumer-facing mobile and web-based fintech apps that enable ACH
3 payments and transfers through consumers' financial accounts (collectively, "Participating
4 Apps"), including popular apps such as Venmo, Coinbase, Square's "Cash App," and Stripe.
5 Venmo had over 52 million active user accounts at the end of 2019;¹⁰ Coinbase reportedly has
6 more than 30 million users;¹¹ and Cash App reportedly has more than 24 million monthly active
7 users.¹² Stripe's payment service reportedly is used by millions of businesses, and thus a
8 commensurate number of consumers.¹³ Plaid's own statistics indicate that Venmo and other
9 payment apps make up over half of fintech app usage.¹⁴

10 **B. Plaid Deceptively Obtains Bank Account Credentials from App Users**

11 22. Plaid has achieved its success by accessing all of the data stored in consumers'
12 financial accounts without consumers' knowledge or consent. The primary service offered by
13 Plaid to the Participating Apps (*i.e.*, apps used by consumers to send and receive money from
14 their financial accounts), is bank "linking" and verification. Verifying that a consumer owns a
15 particular bank account is important for the safety and security of payment transfers using mobile
16 apps. Fintech applications typically verify accounts either by making micro-deposits to a
17 consumer's account, then requiring that the consumer report the amounts back to the app (which
18 can take several days), or by asking a consumer to log in to their bank directly to confirm their
19 identity as an account holder.

20 23. In a typical scenario, consumers log into their banks via an "OAuth" procedure,
21 whereby users are redirected from the original webpage or app directly to their banks. There,
22 consumers log into the bank's webpage or app, and then they are redirected back to the original

23 _____
24 ¹⁰ See <https://investor.paypal-corp.com/static-files/0b7b0dda-a4ee-4763-9eee-76c01be0622c>.

25 ¹¹ See <https://www.coinbase.com/about>.

26 ¹² See <https://www.businessinsider.com/squares-cash-app-reached-24-million-users-and-monetization-surge-2020-2>.

27 ¹³ See <https://www.stripe.com/customers>.

28 ¹⁴ See Oct. 2016 Plaid Publication: *Financial data access methods: Creating a balanced approach*, Appendix C to Plaid's response to CFPB RFI, <https://plaid.com/documents/Plaid-Consumer-Data-Access-RFI-Technical-Policy-Response.pdf>.

1 app.¹⁵ Behind the scenes, the bank returns a “token” that allows the original app to access the
2 consumer’s bank information as necessary and authorized by the consumer, but without giving
3 the app provider access to the login information.

4 24. Plaid has never adhered to the standard and secure OAuth procedure for the critical
5 process of having consumers log into their bank accounts. Instead, for the first several years of
6 Plaid’s operations, Plaid arranged for its fintech clients to collect consumers’ bank login
7 information and then pass that information to Plaid, which then approached the banks directly.¹⁶
8 In or around 2016, Plaid (belatedly, given the security risks) jettisoned this process for one even
9 more beneficial to Plaid.¹⁷

10 25. In or around 2016 Plaid implemented a method to *mimic* the OAuth procedure, but
11 Plaid’s method differs materially from a true OAuth process. Under this current system, Plaid
12 “directly collect[s]” credentials from the consumer. According to Hockey, the goal was not to
13 eliminate the security risk Plaid itself had created, but to “centralize[] that risk” at Plaid.¹⁸

14 26. Plaid refers to this new method as a “Managed OAuth” system. Plaid’s Managed
15 OAuth process has been incorporated in its “Plaid Link” software, which consists of software,
16 including login screens, developed by Plaid and distributed to its fintech clients for incorporation
17 into their apps.¹⁹

18 27. Plaid designs the login screens in its Managed OAuth interface to give them the
19 look and feel of login screens used by individual financial institutions (known as “spoofing”).
20 Because Plaid does not disclose it is not the actual bank, consumers are lulled into a false sense of
21 security by this login process, and this results in increased customer conversion. This process is
22 known as “phishing.”

23
24
25 ¹⁵ See, e.g., <https://www.oauth.com/oauth2-servers/redirect-uris/>.

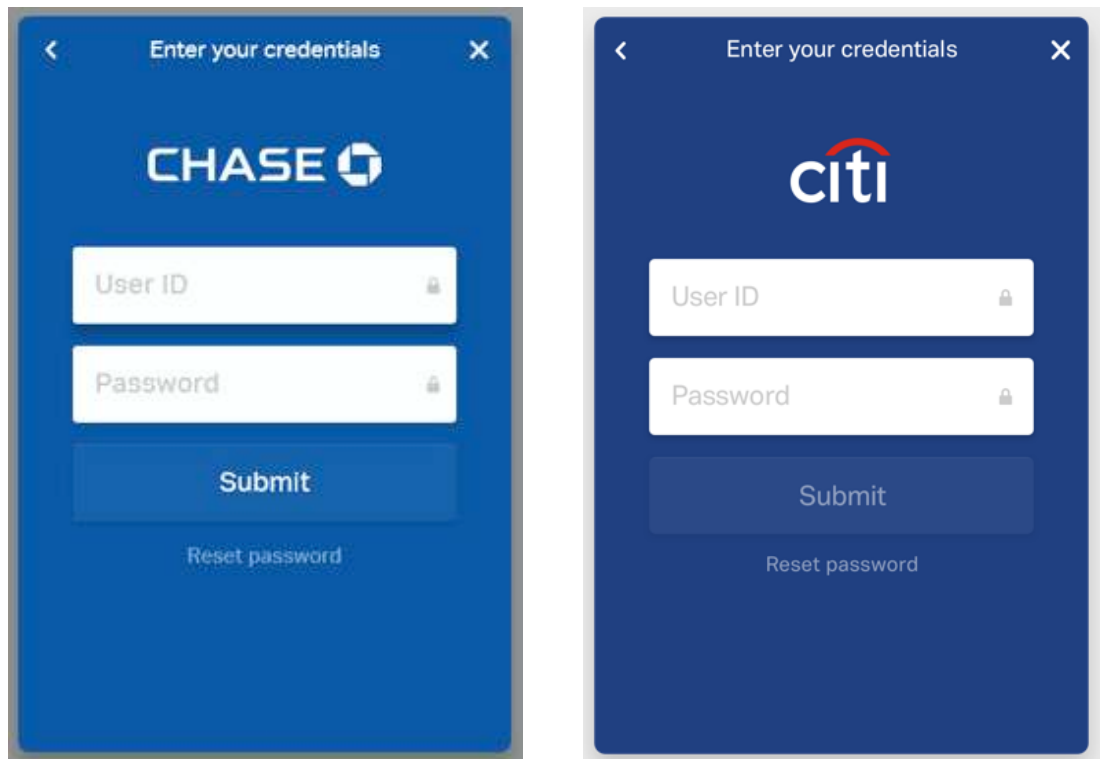
26 ¹⁶ See Sep. 26, 2018 Presentation by William Hockey, *Deep Dive w/ Plaid—William Hockey, Co-
27 Founder & CTO*, at 13:54 to 14:09, <https://www.youtube.com/watch?v=9D5Rwt3DvGg>.

28 ¹⁷ *Id.* at 14:14 to 14:19.

¹⁸ *Id.* at 14:39 to 14:55.

¹⁹ See <https://fin.plaid.com/articles/demystifying-screenless-exchange/>.

1 28. For example, when consumers are prompted to verify their ownership of bank
2 accounts for Venmo using a mobile device or web browser, they are directed to a login screen
3 branded with their chosen bank's logo and color scheme. From a consumer's perspective, the
4 process appears to be the typical OAuth procedure that directs them to their bank to verify the
5 account. Upon selecting a bank, the screen shifts and gives the impression that the user has been
6 directed away from Venmo to interact with another entity, namely, their financial institution. In
7 reality, they have been directed to a connection screen designed and inserted by Plaid *within* the
8 Venmo app, and their communications are to Plaid instead of their trusted financial institution.
9 The following are examples of Plaid's bank-branded login screens viewed in a mobile device:



24 29. On the bank-branded Plaid login screen, consumers enter their login information.
25 Instead of going straight to the bank, as would be the case in an OAuth procedure, the login
26 information instead is transmitted directly to Plaid. Plaid then uses the information to access the
27 consumer's bank account.

28

1 30. Plaid’s use of bank logos and color schemes, and the overall design of the
2 interface, are intentionally deceptive. In April 2016, Plaid’s Charley Ma stated in a comment
3 thread on computer science and entrepreneurship site “Hacker News” that the company had
4 “completely optimized” its “drop-in module used for onboarding bank accounts.”²⁰ A publication
5 for developers on Plaid’s website from later that year sheds light on what this “optimization”
6 entailed. In that publication, Plaid touted how “design elements” in its Managed OAuth process
7 were key to the success of its software in “increasing user conversion,” including by customizing
8 the “look and feel of permissioning access” for financial institutions.²¹ In other words, Plaid
9 specifically designed its system to have the appearance of a redirect-based OAuth system without
10 actually redirecting the consumer to the bank’s website. And Plaid did so for the purpose of
11 ensuring that the look and feel of its process would fool consumers into thinking they were
12 actually logging into their bank rather than realizing that they were handing their login
13 information to a third party.

14 31. In a 2017 blog post directed to its developer client audience, Plaid again conceded
15 that Plaid’s login process was designed to mimic the look and feel of the bank’s website—
16 including through the use of logos and bank-branded color schemes—“so that end-users feel a
17 greater sense of security and familiarity.”²²

18 32. Plaid’s scheme defies industry norms and consumers’ reasonable expectations.
19 This is reflected, among other things, in the reaction of those few members of the app developer
20 community who identified aspects of Plaid’s conduct. For example, in December 2018, Michael
21 Kelly, a Plaid software engineer, was asked by a programmer in a now-deleted thread on Plaid’s
22 GitHub page why Plaid fools users into thinking they are accessing their banks’ websites when
23 logging in through Plaid:

24
25 _____
26 ²⁰ See Jun. 20, 2016 Y Combinator Hacker News thread: *Fintech Firm Plaid Raises \$44M*,
<https://news.ycombinator.com/item?id=11939103>.

27 ²¹ See Nov. 15, 2016 Plaid Article: *Demystifying Screenless Exchange*,
<https://fin.plaid.com/articles/demystifying-screenless-exchange/>.

28 ²² See Dec. 13, 2017 Plaid blog post: *Improving search for 9,600+ banks*,
<https://blog.plaid.com/improved-search/>.

1 [Programmer]: givelively.org prompts me to provide my banking
 2 password on a web donation page. Browser inspector shows it's
 3 putting up a plaid.com iframe. That even renders my bank's logo to
 4 fool me into thinking I'm accessing my bank's site. This is
 5 absolutely unacceptable, regardless of what claims you make on
 6 your security page.

7 [Michael Kelly]: [W]e appreciate your concerns, which is why our
 8 compliance team vets anybody who uses Link. As to malicious
 9 knock offs, this is a matter that most successful companies lookout
 10 for and deal with -- as we and our security team do. If you see
 11 someone impersonating Link in such a way, please drop us a note
 12 at security@plaid.com. It's also worth noting that, in addition to the
 13 security we provide, banks protect their users from credential-based
 14 attacks via multi factor authentication.²³

15 Kelly did not deny that Plaid was spoofing banks' websites, but instead only confirmed Plaid was
 16 aware that malicious parties could try to impersonate Plaid's method for phishing financial
 17 account credentials from fintech app customers.

18 33. Consumers themselves were left in the dark. For example, on a May 2018 Hacker
 19 News thread, Hockey responded to concerns about the collection of bank account transaction data
 20 via Plaid by pointing to whether a fintech app using Plaid (the app Robinhood) was *itself*
 21 collecting the data, thus deflecting awareness of Plaid's own misconduct:

22 [User]: "I would really caution connecting your bank account
 23 through Plaid on [Robinhood]. It's really unclear what data they are
 24 collecting but their privacy policy suggests they are collecting
 25 your bank account transaction history using Plaid's API. 100% a
 26 dealbreaker for me."

27 [Hockey]: "[C]o-founder of Plaid here. I can't give the rationale on
 28 why RH wrote the privacy policy the way they did, but I can
 29 guarantee you that they are not pulling transactional data. They're
 30 only using Plaid for the ACH authentication."²⁴

31 Hockey failed to disclose the vital information that Plaid itself was collecting the banking data
 32 behind the scenes.

33 34. Plaid's conduct is particularly egregious in light of widespread financial industry
 34 recognition that it is improper to ask consumers to share their login information with third parties

35 ²³ See Feb. 11, 2016 Github thread on Plaid "privacy/security concerns,"
 36 <http://web.archive.org/web/20190415103059/https://github.com/plaid/link/issues/68>.

37 ²⁴ See May 13, 2018 Y Combinator Hacker News thread: *Stock-trading app Robinhood was*
 38 *rejected by 75 investors*, <https://news.ycombinator.com/item?id=17060034>.

1 like Plaid. In October 2017, the Consumer Financial Protection Bureau (“CFPB”) released a set
2 of Consumer Protection Principles related to data aggregation services such as those offered by
3 Plaid. The CFPB recognized that one of the core principles for protecting consumers’ banking
4 data where it is being accessed by data aggregators is that such access should not “require
5 consumers to share their account credentials with third parties”—*i.e.*, credentials should not be
6 shared with parties other than the bank. Despite this official guidance, Plaid has persisted with its
7 practice of collecting consumer login information.

8 35. Whether under its original procedure or its even more sophisticated (and
9 deceptive) “Managed OAuth” procedure, Plaid has consistently structured the bank login process
10 in its software to allow it to intercept consumers’ bank login information. As the company
11 admitted in its February 2017 response to the CFPB’s Request for Information (“RFI”) regarding
12 consumer data access, “Plaid has developed a solution that passes credentials directly to the
13 trusted intermediary (Plaid).”²⁵

14 36. In a December 2018 interview, Plaid’s Head of Engineering confirmed that the
15 following description of Plaid’s general method of capturing and using bank login information
16 was “90% accurate”: (1) set up a browser on a virtual machine, (2) have the user go to the bank’s
17 website, (3) have the user put in the banking credentials, and (4) scrape the screen to collect
18 banking data without the user knowing the difference.²⁶ Yet the difference is practically and
19 legally significant: Plaid never had consumers go to the bank’s website, but instead collected their
20 credentials directly.

21 37. Moreover, Plaid fails to properly protect the sensitive login credentials it acquires.
22 Plaid makes partial and deceptive representations to consumers that the software that accesses the
23 bank uses “end-to-end” encryption, thereby ensuring that the user’s login credentials “will never
24 be made accessible” to the Participating App. In reality, Plaid’s method of encryption is far from

25 ²⁵ See Feb. 21, 2017 Response by Plaid to CFPB’s Consumer Data Access RFI,
26 <https://plaid.com/documents/Plaid-Consumer-Data-Access-RFI-Technical-Policy-Response.pdf>,
at 12.

27 ²⁶ See Dec. 13, 2018 Software Engineering Daily Podcast: *Plaid: Banking API Platform with*
28 *Jean-Denis Greze*, <https://softwareengineeringdaily.com/2018/12/13/plaid-banking-api-platform-with-jean-denis-greze/>.

1 secure. Unlike banks and other financial institutions that include a second level of encryption as a
2 standard protection measure for customer login information handled through their apps, Plaid
3 uses a single level of encryption that leaves login credentials open to interception in plain text
4 form by a straightforward method that would be familiar to any malicious actor with even a
5 modicum of decryption expertise. That is, Plaid conceals both the fact of its obtaining banking
6 information, and the ramifications of having it afterwards.

7 **C. Plaid Leverages Credentials to Collect Valuable Data on a Massive Scale**

8 38. Plaid's deception has been successful, and inordinately profitable. By means of the
9 phishing bank login process embedded in the Participating Apps, and by using collected
10 consumer bank login information, Plaid has collected—and now stores, analyzes, and offers to its
11 fintech clients for sale—a staggering amount of consumer banking data.

12 39. Once Plaid captures a consumer's bank login credentials for the ostensible limited,
13 discrete purpose of verifying and linking a user's financial account to their chosen app, it actually
14 uses the credentials to obtain the maximum amount of data accessible to the consumer from the
15 bank. Plaid achieves this by approaching financial institutions under the pretense that Plaid's
16 access is permissioned by their consumer clients, and therefore the institution is legally required
17 by Section 1033 of the Dodd-Frank Act to provide Plaid with *all* available data concerning the
18 accounts in electronic form.²⁷

19 40. From Plaid's earliest days, the company has collected what the co-founders have
20 described as an "immense" amount of consumer spending data and other information from banks.
21 With access to information going back up to five years, Plaid has taken detailed banking
22 information for thousands of transactions for each consumer—3,700 transactions on average—
23 that shows users' healthcare, educational, social, transportation, childcare, political, saving,
24 budgeting, dining, entertainment, and other habits, with an average of 1,750 unique geolocations
25 to which the transactions were mapped.²⁸

26 ²⁷ See May 13, 2019 interview with Zach Perret at Data Driven NYC event at 16:34 to 17:19,
27 <https://www.youtube.com/watch?v=sgnCs34mopw>; see also 12 U.S.C. § 5533 (Dodd-Frank Act
28 Section 1033), which provides for consumer rights "upon request" to access financial account and
account-related data "in electronic form usable by consumers."

²⁸ See Feb. 2013 presentation by Zach Perret and William Hockey at NYC Data Business Meetup

1 41. As a result, even as early as February 2013, Plaid’s co-founders could tell industry
2 insiders that the company was “generating one of the largest transactional data sets in the world.”²⁹

3 42. Plaid generated this data set by engaging in still more unfair and unethical
4 behavior. Plaid circumvented counter-measures employed by some banks to prevent data
5 aggregators like Plaid from siphoning all information in a given consumer’s accounts by
6 accessing accounts with the consumer’s credentials and “scraping” (*i.e.*, copying) data the banks
7 would not share directly. Plaid’s insiders understood the unethical nature of the company’s
8 method of gaining access to banks’ data stores. In August 2018, a former Plaid programmer
9 responded to a Hacker News thread titled, *What is the most unethical thing you've done as a*
10 *programmer?* The programmer identified his work for Plaid as one of the most unethical things
11 he had ever done because, after consumers’ login credentials were obtained, Plaid developed
12 methods for bypassing banks’ protections against data scraping³⁰ by using their status as an
13 “affiliate” of banks’ downstream clients:

14 [Plaid] needed to develop login integrations with consumer banks to
15 acquire customer account information for verification purposes. But
16 many such banks didn’t particularly want to grant them any special
17 API access. More importantly, these banks typically forbid scraping
18 and made it explicitly difficult by implementing JavaScript-based
19 computational measures required on the client in order to
20 successfully login. I helped [Plaid] develop methodologies for
21 bypassing the anti-scraping measures on several banking websites.
22 However, I stopped working on this because 1) I felt uncomfortable
23 with the cavalier way they were ignoring banks’ refusals, then using
24 the reversed integrations and onboarded customers as a bargaining
25 chip for more formal partnerships, and 2) performing huge amounts

26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

29 See <https://news.ycombinator.com/item?id=5304169>.

30 Data scraping is a technique in which a computer program extracts data from human-readable output coming from another program. Normally, data transfer between programs is accomplished using data structures suited for automated processing by computers, not people. The key element that distinguishes data scraping from automated computer data transfer is that the output being scraped is intended for display to an end-user, rather than as input to another program, and is therefore usually neither documented nor structured for convenient parsing. Data scraping is frequently done to interface with a third-party system that does not provide a more convenient API. In this case, the operator of the third-party system will often see screen scraping as unwanted due to, among other reasons, the loss of control of the information content. Consequently, data scraping is generally considered an *ad hoc*, inelegant technique used as a last resort when no other data interchange mechanism is available.

1 of analytics on customer data acquired as part of the account
2 verification process.

3 . . .

4 I don't have an issue with user data being mined for things like
5 market research if it's a situation where the product is free and users
6 can be easily made aware of it. But I find it dishonest if the company
7 mining that data is doing so without direct user consent, or in a
8 "backdoored" manner using their status as a downstream client's
9 "affiliate" for T&C purposes.³¹

10 43. It bears emphasis that if a parent or guardian associates a bank account for their
11 minor child with their own account, such that it is accessible with their own login credentials,
12 even sensitive identifying information about the child would be swept into Plaid's data collection.

13 44. In May 2019, Perret confirmed that the scope of Plaid's data collection had grown
14 to encompass tens of millions of consumers: "The scale has gotten immense. . . . ***About one in***
15 ***four people in the US have linked an account with Plaid***, which means that we're kind of
16 processing all the data coming through all those accounts on the other side."³² The result, Perret
17 explained, was that Plaid is storing what he described as "an immense pile of data," including the
18 raw transactional data collected from banks and the data that Plaid is able to add by way of
19 "enrichment" (e.g., location data that ties the transactions to a vast merchant database Plaid has
20 compiled using that data).³³

21 45. Plaid's Head of Engineering confirmed that the company stores the data it collects
22 for backup purposes, that Plaid is "effectively caching" the banking data, and that it stores raw
23 data in a permanent store.³⁴ As explained by Plaid in its Developer API documentation for app
24 developers, Plaid automatically and consistently updates its cache of consumers' private financial

25 ³¹ See Aug. 5, 2018 Y Combinator Hacker News thread: *What is the most unethical thing you've*
26 *done as a programmer?*, <https://news.ycombinator.com/item?id=17692291>.

27 ³² See May 13, 2019 interview with Zach Perret at Data Driven NYC event at 11:53 to 12:05,
28 <https://www.youtube.com/watch?v=sgnCs34mopw>.

³³ *Id.* at 11:53 to 13:16.

³⁴ See Dec. 13, 2018 Software Engineering Daily Podcast: *Plaid: Banking API Platform with*
Jean-Denis Greze, <https://softwareengineeringdaily.com/2018/12/13/plaid-banking-api-platform-with-jean-denis-greze/>.

1 and identifying information, every few *hours*, regardless of whether the consumer takes any
2 further action:

3 We update a users [sic] account at set intervals throughout the day,
4 independent of how many times a client calls the /connect endpoint.
5 We pull transactions as they are posted to the issuing institution.
6 Dependent on the merchant acquirer, processor, gateway and issuer,
7 the time from when a transaction occurs to when it is posted can
8 take from a couple minutes to a couple days.³⁵

9 46. The information Plaid acquires also is not necessarily limited to data about the
10 individual whose account was initially accessed for purported verification purposes. Once it has a
11 consumer's login credentials, Plaid also pulls *any* transaction, address, contact, and other
12 information in the accounts—whatever is available. Plaid thus also obtains information about any
13 joint account holders, authorized users, and even about related accounts used for a consumer's
14 minor children.

15 47. In the January 13, 2020 press release and accompanying presentation announcing
16 Visa's purchase of Plaid, Visa reiterated that Plaid has the banking information of one in four
17 people with a U.S. bank account, including the banking data from over 200 million accounts.³⁶
18 Venmo users alone accounted for a large portion of those consumers and accounts, given that
19 Venmo had over 52 million users as of the end of 2019.³⁷

20 48. According to the Visa/Plaid press release, Plaid is used by thousands of digital
21 financial apps and services, and accesses data at over 11,000 financial institutions across the
22 U.S., Canada and Europe.³⁸ Indeed, the scale of Plaid's data aggregation is reflected in the
23 magnitude of Visa's purchase price: according to the deal, Visa would pay \$4.9 billion in cash
24 and approximately \$400 million in retention equity and deferred equity.³⁹

25 ³⁵ See <https://plaid.com/docs/legacy/api/>.

26 ³⁶ See Jan. 13, 2020 Press Release: *Visa To Acquire Plaid*, <https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.16856.html>; see also accompanying presentation, https://s1.q4cdn.com/050606653/files/doc_presentations/2020/Visa-Inc.-To-Acquire-Plaid-Presentation.pdf.

27 ³⁷ See <https://investor.paypal-corp.com/static-files/0b7b0dda-a4ee-4763-9eee-76c01be0622c>.

28 ³⁸ See <https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.16856.html>; <https://fortune.com/2020/01/14/visa-plaid-acquisition-fintech/>.

³⁹ See https://s1.q4cdn.com/050606653/files/doc_presentations/2020/Visa-Inc.-To-Acquire-Plaid-

1 **D. Plaid Sells and Otherwise Exploits the Unlawfully-Obtained Private Data**

2 49. Plaid has admitted that it routinely sells the consumer banking data it collects. At a
3 minimum, Plaid sells the data it obtains from consumers' accounts back to the very app providers,
4 including the Participating Apps, who use its services.⁴⁰ Plaid calibrates its prices based on the
5 type of information being sold.⁴¹

6 50. Plaid fails to exercise control or oversight into how these companies store and use
7 the sensitive banking and other private consumer data they purchase from Plaid, or what those
8 companies do with the data after purchasing it. Instead, Plaid purports to rely upon an initial
9 vetting process and a boilerplate Developer Policy with vague terms like "best practices" and
10 "applicable laws": "Your systems and application(s) must handle End User Data securely. With
11 respect to End User Data, you should follow industry best practices Any End User Data in
12 your possession must be stored securely and in accordance with applicable laws."⁴²

13 51. Plaid's vetting process is inadequate to ensure that the thousands of applications
14 paying Plaid for access to the sensitive consumer data it delivers are complying with legal
15 requirements like those imposed by the Gramm-Leach-Bliley Act ("GLBA"). Plaid has no ability
16 to track what companies like the Participating Apps do with the consumer data they purchase
17 from Plaid.

18 52. Plaid also has arranged to sell the vast store of private financial data it possesses to
19 Visa via Visa's purchase of the company for \$5.3 billion.

20 53. In addition to selling raw data, Plaid derives additional valuable benefits for its
21 business by analyzing the private information it obtains from consumers, including by "using
22 machine learning to draw insights about how consumers spend their time, money, and
23

24 _____
[Presentation.pdf](#).

25 ⁴⁰ See Feb. 21, 2017 Response by Plaid to CFPB's RFI, <https://plaid.com/documents/Plaid-Consumer-Data-Access-RFI-Technical-Policy-Response.pdf> (Plaid acknowledges to CFPB that it
26 sells data to party "permissioned" by consumer).

27 ⁴¹ See Feb. 2019 interview with Zach Perret, <https://www.saastr.com/build-a-platform-ecosystem/>.

28 ⁴² See <https://plaid.com/legal/>.

1 attention.”⁴³ In August 2018, a programmer who formerly worked for Plaid confirmed that the
2 company “perform[ed] huge amounts of analytics on customer data acquired as part of the
3 account verification process.” The programmer also highlighted the economic value of the
4 analytics Plaid performs on the banking data, explaining how the data may be monetized by
5 selling the “derivative analytics” of the data to hedge funds, who use the analytics to forecast the
6 revenue of companies in advance of equity earnings announcements.⁴⁴

7 54. As Perret explained in May 2019, Plaid’s long-term business plan is to monetize
8 the mountain of private banking data it has collected. The company is in “phase one,” scaling up
9 its business and gathering and enriching as much information about consumers’ financial and
10 private lives as possible, but ultimately Plaid plans to make a large-scale pivot toward monetizing
11 that data through analytics and the provision of what it calls “value-added services.” As a result,
12 the company employs a large data science team that works on applying sophisticated analytics to
13 the data Plaid has illicitly obtained, with the end goal of developing products for other fintech
14 applications based upon the data and analytics. As Perret put it, over time Plaid’s focus will
15 become “more and more about analytics” (*i.e.*, generating data-based profiles of consumers and
16 their habits) and providing “value-added services on top of the data that’s coming through the
17 system.”⁴⁵

18 55. The data Plaid has accumulated from consumers through material omissions and a
19 series of unfair and unethical actions that invade their privacy has provided the company with a
20 serious competitive advantage. In 2018, Plaid investor Goldman Sachs cited the “sustainable
21 moat or advantage” provided by Plaid’s data network effects, where developers are forced to rely
22 upon Plaid’s technology even to understand their own users’ behavior.⁴⁶

23 _____
24 ⁴³ See Jul. 1, 2015 Y Combinator Hacker News thread,
<https://news.ycombinator.com/item?id=9812245>.

25 ⁴⁴ See Aug. 5, 2018 Y Combinator Hacker News thread: *What is the most unethical thing you've*
done as a programmer?, <https://news.ycombinator.com/item?id=17692291>.

26 ⁴⁵ See May 13, 2019 interview with Zach Perret at Data Driven NYC event at 14:21 to 14:26,
<https://www.youtube.com/watch?v=sgnCs34mopw>.

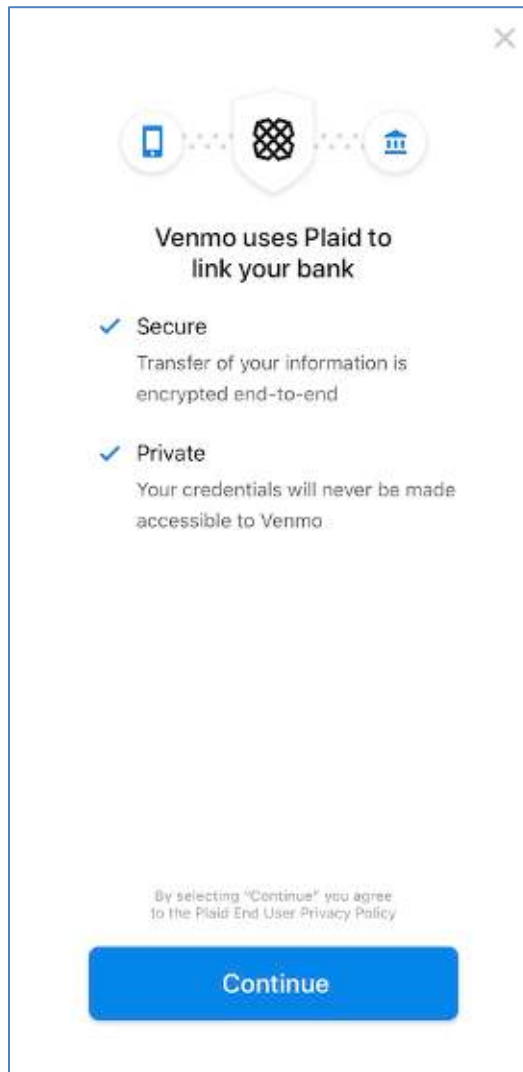
27 ⁴⁶ See Oct. 4, 2018 CNBC article: *Meet the start-up you’ve never heard of that powers Venmo,*
Robinhood and other big consumer apps, [https://www.cnbc.com/2018/10/04/meet-the-startup-](https://www.cnbc.com/2018/10/04/meet-the-startup-that-powers-venmo-robinhood-and-other-big-apps.html)
28 [that-powers-venmo-robinhood-and-other-big-apps.html](https://www.cnbc.com/2018/10/04/meet-the-startup-that-powers-venmo-robinhood-and-other-big-apps.html).

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

E. Plaid and Its Fintech Clients Conceal Plaid’s Conduct from Consumers

56. Plaid distributes to each of its fintech clients a template for use in guiding consumers through the process of linking their financial accounts to the app. Some apps, such as Square’s Cash App, do not even make use of the template and provide no disclosures whatsoever, simply directing consumers to select a bank and input their credentials. In all events, at no time are users of any of the Participating Apps informed that Plaid will receive and retain access to their financial institution account login credentials. Neither are they informed that Plaid or any party would use those credentials to collect information from their financial accounts on the scale and for the duration that actually occurs, let alone that data *not* collected by the fintech clients in the first instance would be made available to them for purchase. Plaid is responsible for ensuring proper disclosures to consumers, both in the content of its own privacy policy and disclosures, and in the privacy-related disclosures in the Plaid software incorporated in the apps of companies through which Plaid interacts with consumers. Plaid has failed to ensure that appropriate disclosures were actually made to consumers using those apps.

1 57. As an illustrative example, when Venmo users are prompted to connect to their
2 bank account in the app, they are directed to the first screen in the Plaid Link software flow,
3 which currently appears as follows:



21 58. The largest text at the top of the screen states, “Venmo uses Plaid to link your
22 bank.” Smaller text underneath states, “Secure: Transfer of your information is encrypted end-to-
23 end,” and underneath that is the assurance: “Private: Your credentials will never be made
24 accessible to Venmo.”

25 59. At the bottom of that screen is a large, bright blue “Continue” button. Just above
26 that button there is text in a still smaller, lighter grey font, stating, “By selecting ‘Continue’ you
27 agree to the Plaid End User Privacy Policy.” There is no visual indication that the latter text is a
28 clickable hyperlink. In fact, however, if the user clicks on that text, they are redirected to Plaid’s

1 privacy policy on its website, located at <http://plaid.com/legal/#end-user-privacy-policy>. The
2 hyperlink is deemphasized in multiple ways, including by failing to underline it (which may
3 signal the presence of a hyperlink), by using a font size that is smaller than text used elsewhere on
4 the screen, and by using a lighter grey color for the text than used elsewhere on the screen, with
5 the lighter grey text set against a light background. As a result, it is not knowable to a reasonable
6 user that the text is a hyperlink unless and until the small text is actually pressed. There are no
7 other elements on the screen directing the user to the existence of the hyperlink. Similarly, there
8 is nothing on this or any subsequent screen that requires the user to actually read through the
9 linked policy, indicate that the terms have been read, or indicate acceptance of the terms of the
10 policy.⁴⁷

11 60. This screen in the Venmo app (which is the same in form, color, and substance for
12 each Participating App except that the name of the app can be customized, as well as whether the
13 blue button says “Continue,” “Ok,” “Get Started,” or “Agree”) contains no description of what
14 Plaid is or what it does, such as a disclosure that Plaid is a completely separate company
15 operating independently of Venmo that intends to establish a long-term connection to the
16 consumer’s bank account and siphon all available private information. There is no indication
17 whatsoever in the app or throughout the process that a Venmo user has gone from interfacing
18 with Venmo to interfacing with any third party other than their own bank.

19 61. In the unlikely event the user sees the fine-print text, decides to test whether it is a
20 hyperlink, and then actually clicks on the link, they are redirected to the beginning of Plaid’s
21 lengthy privacy policy webpage. If the user then takes the time to scroll and read through the
22 policy (although nothing to this point has alerted the user to the possibility that their private data
23 may even be at stake), they will eventually find only this statement:

24 Information we collect from your financial accounts. The
25 information we receive from the financial product and service
26 providers that maintain your financial accounts varies depending on
the specific Plaid services developers use to power their

27 ⁴⁷ Plaid’s privacy policy is no better disclosed to users of other Participating Apps. The screens
28 presented to users of Coinbase, for example, present users with a screen identical in all material
respects as Venmo. Square’s Cash App presents no screen containing reference to “Plaid” or its
privacy policy at all, and simply directs users to a page to “[s]elect [their] bank.”

1 applications, as well as the information made available by those
 2 providers. But, in general, we collect the following types of
 3 identifiers, commercial information, and other personal information
 4 from your financial product and service providers:

- 5 • Account information, including financial institution name,
 6 account name, account type, account ownership, branch
 7 number, IBAN, BIC, and account and routing number;
- 8 • Information about an account balance, including current and
 9 available balance;
- 10 • Information about credit accounts, including due dates,
 11 balances owed, payment amounts and dates, transaction
 12 history, credit limit, repayment status, and interest rate;
- 13 • Information about loan accounts, including due dates,
 14 repayment status, balances, payment amounts and dates,
 15 interest rate, guarantor, loan type, payment plan, and terms;
- 16 • Information about investment accounts, including transaction
 17 information, type of asset, identifying details about the asset,
 18 quantity, price, fees, and cost basis;
- 19 • Identifiers and information about the account owner(s),
 20 including name, email address, phone number, date of birth,
 21 and address information;
- 22 • Information about account transactions, including amount,
 23 date, payee, type, quantity, price, location, involved securities,
 24 and a description of the transaction; and
- 25 • Professional information, including information about your
 26 employer, in limited cases where you've connected your
 27 payroll accounts.

28 The data collected from your financial accounts includes
 information from all your accounts (e.g., checking, savings, and
 credit card) accessible through a single set of account credentials.⁴⁸

62. Plaid's software incorporated in the Venmo app is illustrative of the way Plaid
 conceals the true facts from consumers:

a. The manner in which Plaid's software is incorporated into the Venmo app is not
 fully disclosed, and, more importantly, nowhere is it disclosed that Plaid uses bank login
 information to access consumers' accounts.

⁴⁸ See Plaid Privacy Policy, <https://plaid.com/legal/#end-user-privacy-policy> (emphasis added).
 See *infra*, Section V.G.3, for further discussion of these terms.

1 b. Multiple statements in the Plaid software incorporated in the Venmo app have a
2 tendency to deceive. Users are told they need to “sign in” to their bank accounts. They receive
3 promises that the system is “Private,” and that the consumer’s “credentials will never be made
4 accessible to Venmo.” In fact, the system is designed not to be private because it requires passing
5 credentials to Plaid as a third-party data aggregator and also includes the wholesale looting of the
6 consumer’s most private banking data. By stating that the login credentials will not be made
7 accessible to Venmo, consumers are falsely led to reasonably expect that their credentials are not
8 shared at all during the account verification process, other than with the bank they know and
9 trust, while in fact those credentials are intercepted by Plaid for its use in gathering data from the
10 bank. In addition, Plaid’s failure to implement a second level of encryption, consistent with the
11 practice of legitimate financial institutions, leaves consumer credentials vulnerable to
12 interception in plain text form by malicious actors with even minimal decryption expertise.

13 c. Another statement in the Plaid software incorporated in the Venmo app that is
14 deceptive on its own and relevant for what it does *not* disclose is the promise that the system is
15 “Secure,” and that the consumer’s information is “encrypted end-to-end.” In fact, the system is
16 designed not to be secure, including because: (i) Plaid uses it to collect, sell, use, and store
17 consumers’ most private financial data; (ii) Plaid fails to exercise control or oversight over how
18 that data is stored or used after it sells it to Venmo; and (iii) when Plaid removes consumer
19 banking data from the secure banking environment, it thereby destroys valuable protections
20 afforded to consumers in the event of data breach or theft. And by stating that the consumer’s
21 information is encrypted end-to-end, consumers are falsely led to believe that no entity outside of
22 Venmo and the bank ever receives access to any consumer information. In addition, Plaid’s
23 failure to implement an industry-standard second level of encryption renders its system unsecure
24 by leaving consumer credentials vulnerable to interception in plain text form by malicious actors
25 with even minimal decryption expertise.

26 d. Plaid’s practice of spoofing bank login websites in its software—including
27 without limitation by the design, context, and performance of the application—deceives
28 consumers as to the existence of Plaid as a separate entity, Plaid’s status as a third party, the fact

1 that Plaid collects consumer bank login information directly, and the fact that Plaid uses bank
2 login information to access consumers' accounts. It instead is intended to deceive consumers into
3 believing that they are entering their bank login directly at the bank's website, as would be the
4 case in a standard, redirect-based OAuth procedure.

5 e. The link in the Venmo app to Plaid's privacy policy is deemphasized and hidden
6 from the consumer's attention, including through its placement; the size and color of the font
7 used; the lack of underlining or other means of notifying the consumer that the text is actually a
8 hyperlink; the reasonable expectation a consumer would have about the level of disclosure that
9 would be provided in advance of divulging sensitive financial data to a third party; and, by
10 contrast, the diminutive nature of the text used for the hyperlink as compared to other text and
11 other surrounding elements incorporated on the screen.

12 f. The Plaid software incorporated in the Venmo app fails to require affirmative
13 consumer permission for Plaid to access, sell, use or store any consumer banking information.

14 g. The Plaid software incorporated in the Venmo app uses a "fine-print click-
15 through" disclosure process that is inadequate to establish knowledge or consent to Plaid's
16 practices by consumers, even if the policy itself had fully and sufficiently disclosed Plaid's true
17 conduct (which it did not).

18 h. Plaid's privacy policy fails to disclose the following facts: (i) Plaid collects
19 consumer bank login information directly; (ii) Plaid uses bank login information to access
20 consumers' accounts; (iii) Plaid collects all available private financial and other identifying data
21 from every available account once it accesses the "linked" account; (iv) Plaid sells the consumer
22 banking data it collects to its clients; (v) Plaid does not exercise adequate oversight over how
23 consumer banking data is stored or used after it sells that data to Venmo; (vi) Plaid otherwise
24 uses and monetizes the consumer banking data it collects; (vii) Plaid stores the consumer
25 banking data it collects; (viii) Venmo purchases, uses, and stores the consumer banking data
26 collected by Plaid; (ix) Plaid continues to access accounts and collect, sell and use consumer
27 banking data after the initial connection is made, regardless of whether the consumer continues
28 using the Venmo app; and (x) by removing consumer banking data from the secure banking

1 environment, Plaid is destroying valuable protections afforded to consumers in the event of data
2 breach or theft.

3 i. Plaid falsely implies limitations to its data aggregation practices in its privacy
4 policy in stating that the information it gathers from financial institutions “varies depending on
5 the specific Plaid services developers use to power their applications.” In fact, Plaid collects all
6 available consumer banking information when it connects with a consumer’s account, whether or
7 not Venmo ultimately requests its own access to the data, and regardless of whether the data has
8 any relevance to transactions on Venmo. The most basic Plaid “tier” for app developers always
9 includes Plaid’s “Transactions” product (*i.e.*, the option to access years of historical account
10 activity), for example, because Plaid collects all transaction information as a matter of course.⁴⁹

11 j. By Plaid stating in its privacy policy that the company collects “[i]nformation
12 about account transactions, including amount, date, payee, type, quantity, price, location,
13 involved securities, and a description of the transaction,” Plaid deceives consumers who use
14 Venmo into believing that it only collects information about transactions conducted using the
15 Venmo app. Plaid thereby conceals the fact that it collects years’ worth of transaction
16 information entirely unrelated to the consumer’s use of Venmo.

17 63. Plaid designs and employs its software to ensure that none of the Participating
18 Apps disclose Plaid’s conduct described herein to consumers.

19 64. As a result of Plaid’s inadequate and misleading disclosures, consumers have been
20 kept in the dark about the role Plaid plays in the relationship between consumers, fintech apps,
21 and financial institutions. Indeed, it was Plaid’s plan from the beginning, as Hockey explained,
22 that “most people will never know we exist.”⁵⁰ And in a 2019 interview, Perret confirmed that
23 Plaid believes consumers “never need to know” they are using Plaid, and Plaid doesn’t “need
24 every consumer to know who Plaid is”; to the contrary, the only thing Plaid wants consumers to
25

26 _____
27 ⁴⁹ See <https://plaid.com/pricing/>.

28 ⁵⁰ See Aug. 2013 emorywire article: *To Hack and Disrupt*,
http://www.alumni.emory.edu/emorywire/issues/2013/august/of_interest/story_1/index.html#.Xk sqMxNKjQg.

1 know is that they are using a fintech app.⁵¹ The vast majority of consumers therefore have no idea
 2 that Plaid even exists, much less that it has collected, stored, sold, and is using their most
 3 sensitive and private financial information.

4 65. In an October 2018 article on Plaid, CNBC reported that “[d]espite popularity with
 5 coders, the average person interacting with Plaid most likely wouldn’t recognize the company”
 6 and the fact that it “quietly powers” Venmo and many other apps. The article also reveals that
 7 Plaid’s largest investors were well aware that consumers have no idea about Plaid or its role with
 8 those apps: “‘Plaid has quietly created a very big infrastructure *without the consumer knowing*
 9 *that they’re powering it,*’ said Christopher Dawe, co-head of private investment at Goldman
 10 Sachs Investment Partners . . . , who led Goldman’s 2016 Series B investment in Plaid”⁵²

11 **F. Plaid’s Harm to Consumers is Recognized by Banks and Industry Groups**

12 66. Because of Plaid’s deficient disclosures and active concealment of the true state of
 13 affairs, consumers using the Participating Apps are unaware that their financial data has been
 14 extracted, analyzed, and sold by Plaid. Banks and other sophisticated industry groups, however,
 15 have been rightfully concerned about the actions of data aggregators like Plaid for some time. In
 16 JPMorgan Chase’s April 2016 shareholder letter, for example, the CEO stated that the bank had
 17 analyzed many third-party contracts providing consumer banking data access to outside entities
 18 such as payment providers and data aggregators. The bank concluded that: (1) “[f]ar more
 19 information is taken than the third party needs in order to do its job”; (2) “[m]any third parties sell
 20 or trade information in a way customers may not understand, and the third parties, quite often, are
 21 doing it for their own economic benefit – not for the customer’s benefit”; and (3) “this is being
 22 done on a daily basis for years after the customer signed up for the services, which they may no
 23 longer be using.” He also stated: “When customers give out their bank passcode, they may not
 24 realize that if a rogue employee at an aggregator uses this passcode to steal money from the
 25

26 ⁵¹ See Feb. 2019 interview with Zach Perret at 19:08 to 19:37, <https://www.saastr.com/build-a-platform-ecosystem/>.

27 ⁵² See Oct. 4, 2018 CNBC article: *Meet the start-up you’ve never heard of that powers Venmo, Robinhood and other big consumer apps*, <https://www.cnbc.com/2018/10/04/meet-the-startup-that-powers-venmo-robinhood-and-other-big-apps.html> (emphasis added).
 28

1 customer's account, the customer, not the bank, is responsible for any loss. . . . This lack of clarity
2 and transparency isn't fair or right."⁵³

3 67. In February 2017, the American Bankers Association provided a response to the
4 CFPB's RFI, identifying numerous concerns and issues with the practices of data aggregators
5 such as Plaid, including the following:

6 (a) Unknowing Grant of Unlimited Access

7 "Current practices in the data aggregation market . . . may leave
8 consumers exposed and create risk that undermine this trust.
9 Consumers today are offered a Faustian bargain in which their
10 desire for technology-driven convenience is exchanged—often
11 unknowingly—for increased potential of catastrophe, by handing
12 over the keys to their financial vault. When consumers share their
13 login credentials with an aggregator, they are giving the aggregator
14 *carte blanche* access to their financial data, including information
15 about things such as their life savings or retirement account. Yet
16 consumers are not given adequate information or control over what
17 information is being taken, how long it is accessible, and how it
18 will be used in the future."⁵⁴

14 (b) Unknowing Removal of Sensitive Information from Secure
Environment

15 "Moreover, consumers are unaware of the differences in the legal
16 and supervisory standards applicable to bank and nonbank
17 participants in the financial services marketplace. Once the
18 information is shared, it leaves a secure bank environment, where it
19 is accorded longstanding legal protections, and it is released into the
20 data services market where it is accorded no more special status
21 than data created through a consumer's use of a social media
22 platform.

23 . . .

24 When consumers allow data aggregators to access their data they run
25 the risk – often unknowingly – associated with moving their data out
26 of the secure banking environment, where it is fully protected by law,
27 and moving it into the data services market where it is not accorded
28 appropriate protections. More troubling is that a number of these non-
bank consumer financial data service providers take the position that
financial data are no different from any other form of data, and as

53 See Apr. 6, 2016 Letter from JPMorgan Chase to shareholders,
<https://www.jpmorganchase.com/corporate/annual-report/2015/>.

54 See Feb. 21, 2017 Response by American Bankers Association to CFPB RFI,
<https://buckleyfirm.com/sites/default/files/Buckley%20Sandler%20InfoBytes%20-%20American%20Bankers%20Association%202017.02.21%20Comment%20Letter%20to%20CFPB%27s%20RFI%20CFPB-2016-0048.pdf>.

1 such ignore or avoid any protections that should be afforded it.
 2 Furthermore, the lack of transparency and control, and the liability
 3 limits asserted by the aggregator, all work to the consumer's
 4 disadvantage."⁵⁵

4 (c) Access Unlimited as to Scope or Time

5 "Today, when consumers provide their access credentials to a data
 6 aggregator, they are giving that company access to any information
 7 that is housed in their online bank account, and they give access for
 8 an unlimited period of time. There is little effort to inform consumers
 9 about the information being taken, how it is being used or shared,
 10 how often it is being accessed, and how long the aggregator will
 11 continue to access it."⁵⁶

9 (d) Access to Unnecessary Data

10 "Consumers assume that data aggregators take only the data needed
 11 to provide the service requested. However, too often it is not the
 12 case."⁵⁷

13 (e) Use and Sale of Banking Data

14 "Many data aggregators use the data for purposes beyond the specific
 15 service that the customer sought. Access to all data enables the
 16 aggregator to profit by selling the information to other third parties
 17 even though the customer neither knew about that potential use nor
 18 requested any additional services or marketing."⁵⁸

17 (f) Increased Risk of Identity Theft

18 "The risks to consumers should not be minimized. First, the sheer
 19 volume and value of the aggregated data make data aggregators a
 20 priority target for criminals, including identity thieves. This is
 21 because data aggregators collect and share information from multiple
 22 financial institutions which is a vast expansion of the information
 23 held at any one bank. Thus, data aggregators may have the financial
 24 information, including account credentials, for the accounts across a
 25 consumer's entire financial portfolio. Through a single source, the
 26 criminal may gain access to the consumer's checking and savings
 27 accounts, retirement accounts, certificates of deposits, credit cards,
 28 brokerage accounts, and insurance products. Also, increasingly data
 aggregators have the ability to conduct transactions, such as sending
 remittances, on behalf of consumers. This rich reward for a single

26 ⁵⁵ *Id.*

27 ⁵⁶ *Id.*

28 ⁵⁷ *Id.*

⁵⁸ *Id.*

1 hack, either of an aggregated database of personally identifiable
2 information or of a single consumer’s multiple accounts, makes data
3 aggregators an attractive target for criminals. They obtain the key not
4 to just a single room, but the key ring with keys to all the rooms.

5 [T]he impact on the consumer in the event of a compromise can be
6 far greater than a single-financial institution compromise. With the
7 consumers’ credentials and account information, criminals may drain
8 deposit accounts, liquidate stocks, and max out credit cards. Even if
9 consumers are ultimately reimbursed, they may suffer crippling
10 inconvenience from even a temporary loss of access because the
11 unauthorized access involves all their financial accounts. They may
12 have no access to funds for day-to-day living. Important payments
13 may be returned unpaid, stocks may be sold at disadvantageous
14 prices, and schedules and peace of mind will be upended as they
15 attempt to recover their assets.”⁵⁹

16 68. Some banks have rightly rejected Plaid’s assertions that consumers authorize its
17 conduct, and have taken extreme measures to protect their customers from Plaid. In December
18 2019, the Wall Street Journal reported on PNC Bank’s actions in upgrading its security systems to
19 prevent Plaid from accessing its banking customers’ information for Venmo and other apps.
20 PNC’s head of retail banking, Karen Larrimer, was quoted in the article as justifying the bank’s
21 actions based upon Plaid’s storage of account access information “indefinitely, often
22 unbeknownst to customers,” putting customers and their money at risk.⁶⁰

23 69. Larrimer further explained in a subsequent article that PNC’s position is that many
24 consumers do not fully understand what happens to their data when they sign up for an app, and
25 an aggregator such as Plaid is involved behind the scenes. One thing many consumers do not
26 recognize, Larrimer explained, is that once access has been obtained to one banking account, the
27 aggregator “can scrape every piece of information that is in your banking relationships—any
28 other accounts you have, any loans you have, any transaction data, whatever is there they have
29 full access to.” Larrimer also explained that the bank was concerned about lack of consumer

⁵⁹ *Id.*

⁶⁰ See Dec. 14, 2019 Article: *Venmo Glitch Opens Window on War Between Banks, Fintech Firms*, <https://www.wsj.com/articles/venmo-glitch-opens-window-on-war-between-banks-fintech-firms-11576319402>.

1 knowledge of where their data is being stored, for how long it is stored, or for what purposes it is
2 being used.⁶¹

3 70. These concerns raised by banks and industry groups are valid. Plaid collects, sells,
4 and uses the most sensitive consumer banking data on a shockingly large scale by employing its
5 Managed OAuth procedure and hiding its activity from consumers.

6 **G. Plaid Knowingly Violates Established Industry Standards and Obligations**

7 71. Plaid's omissions, non-disclosures, misdirection, and active concealment
8 represented in Plaid's statements described herein; throughout the template-based account
9 verification and linking process; throughout Plaid's process for obtaining information about
10 consumers from their financial accounts; and in Plaid's use, analysis, and sale of that information
11 and insights derived from it, all violate consumers' reasonable expectations and industry norms.
12 This conduct by Plaid also violates established industry standards and Plaid's obligations under
13 the GLBA (Section G.1). Plaid acknowledges these standards and its responsibilities under the
14 GLBA (Section G.2), but, in practice, Plaid violates those standards along with consumers'
15 reasonable expectations founded thereupon (Section G.3). Plaid's deceptive conduct and
16 omissions are intentional.

17 **1. The GLBA Standards**

18 72. Plaid is a financial institution subject to the GLBA and the regulations
19 promulgated thereunder, including Privacy of Consumer Financial Information (the "Privacy
20 Rule"), 16 C.F.R. Part 313, recodified at 12 C.F.R. Part 1016 ("Reg. P"), and issued pursuant to
21 the GLBA, 15 U.S.C. §§ 6801-6803. The Privacy Rule and Reg. P hold financial institutions to an
22 elevated standard with regard to the privacy notices that must be provided to their customers.

23 Among other things:

24 a. Privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5;
25 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably
26

27
28 ⁶¹ See Jan. 2020 Article: *PNC Bank Counters 'P2P War' Speculation Over Its Venmo App Moves*,
<https://thefinancialbrand.com/91550/pnc-bank-p2p-venmo-mobile-app-zelle-plaid-aggregator/>.

1 understandable and designed to call attention to the nature and significance of the information in
2 the notice.” 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1).

3 b. Privacy notices must “accurately reflect[.]” the financial institution’s privacy
4 policies and practices. 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. The
5 notices must include the categories of nonpublic personal information the financial institution
6 collects and discloses, the categories of third parties to whom the financial institution discloses
7 the information, and the financial institution’s security and confidentiality policies. 16 C.F.R.
8 § 313.6; 12 C.F.R. § 1016.6.

9 c. Privacy notices must be provided “so that each consumer can reasonably be
10 expected to receive actual notice.” 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. For the consumer who
11 conducts transactions electronically, the financial institution must (1) “clearly and
12 conspicuously” post the notice on an electronic site, and (2) “require the consumer to
13 acknowledge receipt of the notice as a necessary step to obtaining a particular financial product
14 or service.” 16 C.F.R. § 313.9(b)(1)(iii); 12 C.F.R. § 1016.9(b)(1)(iii).

15 73. Consistent with the requirements under the GLBA, the CFPB’s October 2017
16 Consumer Protection Principles provide that the terms of access, storage, and use of consumer
17 data must be “fully and effectively disclosed to the consumer, understood by the consumer, not
18 overly broad, and consistent with the consumer’s reasonable expectations in light of the
19 product(s) or service(s) selected by the consumer.” In addition, data access terms must address
20 “access frequency, data scope, and retention period.” Further, consumers must be informed of any
21 third parties that access or use their information, including the “identity and security of each such
22 party, the data they access, their use of such data, and the frequency at which they access the
23 data.”⁶²

24
25
26
27 ⁶² See Oct. 18, 2017 CFPB release: *Consumer Protection Principles: Consumer-Authorized*
28 *Financial Data Sharing and Aggregation*,
[https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-
aggregation.pdf](https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf).

1 2. **Plaid’s Acknowledgement of Its Disclosure Obligations**

2 74. Plaid is well aware of its disclosure obligations and has consistently held itself up
3 as a paragon of consumer disclosure. For example, in an October 2016 publication, Plaid took the
4 position that “[d]ata collection and retention policies should be clearly displayed in plain English
5 to consumers by permissioned parties, typically during onboarding – in other words,
6 *transparency is critical.*”⁶³

7 75. Plaid has admitted its privacy policy is subject to the Privacy Rule’s “clear and
8 conspicuous” requirement. Plaid also has recognized its responsibility for ensuring that the
9 relevant privacy notices in the Participating Apps meet those requirements. For example, the 2016
10 version of Plaid’s “Legal” page pays lip-service to the requirements with the following statement
11 in its developer-facing “Terms of Use”:

12 Your product must maintain a *clear and conspicuous link in its*
13 *privacy policy to Plaid’s Privacy Policy.* Such link must include a
14 *clear and conspicuous statement* that each end user acknowledges
15 and agrees that information will be treated in accordance with such
16 policy. . . . All of the foregoing must be done in a form and manner
17 that is acceptable to Plaid. You will immediately make any changes
18 requested by us.⁶⁴

19 76. Plaid similarly acknowledges that the data it transfers to the Participating Apps is
20 subject to another aspect of the GLBA, the “Safeguards Rule” (16 C.F.R. Part 314). Plaid’s
21 “Developer Policy” states: “Your systems and application(s) must handle End User Data securely.
22 With respect to End User Data, you should follow industry best practices but, at a minimum, must
23 . . . [c]omply with *relevant rules and regulations* with regard to the type of data you are
24 handling, *such as the Safeguards Rule.*”⁶⁵

25 77. In its February 2017 response to the CFPB’s RFI, Plaid stated:

26 An existing legal framework – the Gramm-Leach-Bliley Act
27 (GLBA) – governs the proper disclosure and use of consumer
28 financial data. Ecosystem participants – both traditional institutions

26 ⁶³ See Oct. 2016 Plaid Publication: *Financial data access methods: Creating a balanced*
27 *approach*, Appendix C to Plaid’s response to CFPB RFI, <https://plaid.com/documents/Plaid-Consumer-Data-Access-RFI-Technical-Policy-Response.pdf> (emphasis added).

27 ⁶⁴ See <https://web.archive.org/web/20160920005638/https://plaid.com/legal/> (emphasis added).

28 ⁶⁵ See <https://plaid.com/legal/>.

1 and newer digital players – should abide by this framework,
 2 including provisions that limit the use of permissioned data to the
 3 scope of the consumer’s consent. More generally, the disclosure
 and use of consumer data by digital products and services is subject
 to all applicable laws and regulations.

4 . . .

5 Beyond the letter of the law, both intermediaries and permissioned
 6 parties should also honor the principles of data minimization and
 consumer transparency. Consumers should know what data is being
 7 collected, and for how long it may be stored. . . . Permissioned
 parties and trusted intermediaries should clearly disclose terms of
 data collection policies to consumers.”⁶⁶

8
 9 78. In a March 2019 letter to the U.S. Senate, Plaid described its approach to data
 10 access as founded firmly in *affirmative consumer permission*:

11 Plaid represents a new approach enabled by modern technology,
 helping a consumer access their own data only when they chose to
 12 do so, and sharing it only with the companies they select. This is a
 consumer-permissioned model, in which consumers control what
 13 they do with their data.

14 Consumer permission is the backbone of account connectivity.
 However, industry disclosure practices can and should be
 15 improved. At Plaid, consumer permission and control are core
 principles. Unlike many other service providers who rely on
 16 personal or financial data, our account connectivity services require
 consumers to affirmatively provide or permission access to their
 17 account information to the company they want to share it with.

18 Most importantly, consumers should understand: What data is
 being shared? For what purpose? And what ability do they have to
 19 direct what happens to their data? At Plaid, we have developed
 simple, plain-English disclosures and privacy policies designed to
 20 help consumers understand which information is collected and how
 it is used, shared and stored. We have previously discussed the
 21 potential benefits of Schumer-box⁶⁷-like disclosures for consumer
 data access, and believe Plaid—and the rest of the industry—should
 22 continue to develop and test more effective consumer disclosures.

23 [C]onsumer permission should be tied to the services the consumer
 requests or purposes for which they are specifically informed when

24
 25 ⁶⁶ See Feb. 21, 2017 Response by Plaid to CFPB’s Consumer Data Access RFI,
<https://plaid.com/documents/Plaid-Consumer-Data-Access-RFI-Technical-Policy-Response.pdf>
 (emphasis added).

26 ⁶⁷ A Schumer Box, named after Senator Chuck Schumer, is an easy-to-read table or “box” that
 27 discloses the rates, fees, terms and conditions of a credit card agreement as required under
 the federal Truth in Lending Act. It requires that all credit card companies use the same
 28 standardized format and font sizes to disclose certain aspects of a credit card agreement so
 consumers can easily understand and compare rates and fees associated with a credit card.

1 they grant access. Affirmative permission (not fine-print click-
 2 through) should be required in order to sell account data, even in
 3 aggregated form, to any parties the consumer doesn't have a direct
 4 permissioning relationship with. To do otherwise would breach the
 5 trust consumers place in fintech providers. Static disclosure, such as
 a Schumer box when initially seeking customer consent, is
 important. But ongoing control will require development of more
 dynamic controls, which should give consumers the ability to
 manage their data.⁶⁸

6 In this letter, Plaid acknowledged: (a) how critically important it is for consumers to understand at
 7 the outset how their data is being accessed, used, shared, and stored; (b) the important role
 8 disclosures and privacy policies play in ensuring such understanding; (c) that consumer
 9 disclosures must be clear, plainly written, and easily understandable; (d) that consumer
 10 permission must be tied to the purpose for which they are granting access to their data; (e) that
 11 affirmative permission, and not "fine-print click-through," is the proper standard for obtaining
 12 consumer permission; (f) that static disclosures are not enough; and (g) that for static disclosures
 13 to be effective at all, they should mirror the form of the "Schumer box" used to disclose the terms
 14 for credit card agreements as mandated under the federal Truth in Lending Act.

15 79. Perret similarly has said that it is "really important" for consumers using Plaid's
 16 software to understand things like "data privacy, where their data is going, [and] how it's
 17 going."⁶⁹

18 **3. Violations of GLBA Standards in Plaid's Privacy Policy**

19 80. Plaid's acknowledgements of its responsibilities to consumers and obligations
 20 under the GLBA are not consistent with Plaid's actual practices. Plaid's privacy policy—
 21 accessible only in the small, greyed out hyperlink in Plaid's template consumer interface pictured
 22 above—is not meaningfully presented to Plaintiffs and Class members. Even if a consumer
 23 somehow became aware of the "policy," the privacy-related purported disclosures knowingly and
 24 intentionally violate the requirements of the Privacy Rule and Reg. P under the GLBA. By way of
 25

26 _____
 27 ⁶⁸ See Mar. 15, 2019 Letter from Plaid to U.S. Senate,
https://www.banking.senate.gov/imo/media/doc/Data%20Submission_Plaid1.pdf.

28 ⁶⁹ See May 13, 2019 interview with Zach Perret at Data Driven NYC event at 21:38 to 26:11,
<https://www.youtube.com/watch?v=sgnCs34mopw>.

1 example, Plaid’s template presented to consumers, discussed and illustrated above with respect to
2 the Venmo app, violates these standards for the following reasons, without limitation:

3 a. Plaid’s privacy policy is not “clear and conspicuous” because the text used in
4 Plaid’s software to link to its privacy policy (the “prompting text”) is not “designed to call
5 attention” to the existence of the notice itself. 16 C.F.R. § 313.3(b)(1). Plaid failed to meet that
6 standard because, among other reasons, it (a) did not “[u]se a plain-language heading to call
7 attention to the notice,” but rather simply included a link in a sentence above the “Continue”
8 button (16 C.F.R. § 313.3(b)(2)(ii)(A)); (b) did not “[u]se a typeface and type size that are easy
9 to read,” but rather used the smallest and lightest font on the screen (16 C.F.R.
10 § 313.3(b)(2)(ii)(B)); (c) did not “[u]se boldface or italics for key words,” but rather made the
11 hyperlink the same font as the surrounding text (16 C.F.R. § 313.3(b)(2)(ii)(D)); and (d) did not
12 “use distinctive type size, style, and graphic devices, such as shading or sidebars,” when
13 combining its notice with other information. 16 C.F.R. § 313.3(b)(2)(ii)(E).

14 b. Plaid’s privacy policy is not “clear and conspicuous” because the prompting text
15 is not “designed to call attention” to the “nature and significance of the information” in the
16 notice. 16 C.F.R. § 313.3(b)(1). Plaid failed to meet that standard because nothing in the
17 prompting text calls attention to the nature or significance of the information in the notice. That
18 screen of Plaid’s software contains no indication, for example, that Plaid is a third party; that
19 Plaid will collect the user’s private bank login information itself; or, critically, that Plaid will
20 access, collect, transfer, sell, use, or store the entirety of personal information available from the
21 user’s bank, including years of transactional banking data from all linked accounts. Plaid was
22 required to make that information “reasonably understandable” by, for example, presenting the
23 information in “clear, concise sentences.” 16 C.F.R. § 313.3(b)(2)(i)(A).

24 c. Plaid’s privacy policy is not “clear and conspicuous” because the policy is not
25 “designed to call attention” to the “nature and significance of the information” therein. 16 C.F.R.
26 § 313.3(b)(1). Among other things, Plaid’s privacy policy fails to explain that Plaid will access,
27 collect, transfer, sell, use, or store the entirety of personal information available from the user’s
28 bank, including years of transactional banking data from all linked accounts. In addition, by

1 using non-specific, misleading statements about Plaid collecting “transactional information,”
 2 Plaid fails to “[a]void explanations that are imprecise and readily subject to different
 3 interpretations.” 16 C.F.R. § 313.3(b)(2)(i)(F).

4 d. Plaid’s privacy policy is not “clear and conspicuous” because the prompting text
 5 is not placed on a screen in the Venmo app (or any Participating App) that consumers
 6 “frequently access,” and—for the reasons described above—is not “labeled appropriately to
 7 convey the importance, nature and relevance of the notice.” 16 C.F.R. § 313.3(b)(2)(iii). In
 8 addition, Plaid’s screen is not designed to ensure that other elements “do not distract from the
 9 notice.” *Id.*

10 e. Plaid’s privacy policy does not “accurately reflect[]” its actual policies and
 11 practices. 16 C.F.R. §§ 313.4 and 313.5. Plaid’s privacy policy fails to explain that Plaid will
 12 access, collect, transfer, sell, use, or store the entirety of personal information available from the
 13 user’s bank, including years of transactional banking data from all linked accounts. Rather, by
 14 using non-specific, misleading statements about Plaid collecting “transactional information,”
 15 Plaid obscures the true nature of its practices.

16 f. Plaid’s privacy policy is not provided “so that each consumer can reasonably be
 17 expected to receive actual notice.” 16 C.F.R. § 313.9. As discussed above, Plaid did not “clearly
 18 and conspicuously” post its policy for its users, all of whom conduct transactions electronically.
 19 16 C.F.R. § 313.9(b)(1)(iii). Neither does Plaid “require the consumer to acknowledge receipt of
 20 the notice as a necessary step to obtaining a particular financial product or service.” *Id.*

21 **VI. INJURY AND DAMAGES TO THE CLASS**

22 81. As Participating App users who linked their financial accounts using Plaid’s
 23 software integrated with the app, Plaintiffs and all other Class members have suffered egregious
 24 invasions of privacy, violations of their dignitary rights, and significant economic damages as a
 25 direct result of Plaid’s misconduct.

26 **A. The Named Plaintiffs’ Experiences**

27 82. Plaintiff **James Cottle** signed up to use the Venmo app in or about January 2019
 28 via his mobile phone. When Mr. Cottle established his account with Venmo, he did so for the

1 purpose, consistent with the services offered by Venmo, of being able to send and receive
2 payments to or from friends, vendors, acquaintances, and other consumers.

3 83. Mr. Cottle does not recall specific details regarding the process of logging into his
4 bank account in the Venmo app so that he could send and receive money through the app. He
5 does not recall being prompted to read any privacy policy during the process of logging into his
6 bank account and does not recall having ever read any privacy policy from Venmo or Plaid when
7 he linked his bank account. He does not recall being sent any privacy policy after signing up, or
8 subsequently seeing any updates to a privacy policy related to his Venmo account or its
9 connection to his bank account.

10 84. At the time Mr. Cottle established his account with Venmo, he was not aware of
11 the existence or role of Plaid. When he was prompted in the Venmo app to log into his bank
12 account, he believed he was doing so through an official connection with his bank. He was
13 unaware that he was providing his login credentials to Plaid.

14 85. When Mr. Cottle was prompted in the Venmo app to log into his bank account, he
15 was not aware that Plaid: (a) would collect any of his banking information as part of that process;
16 (b) would collect, receive, or store any of his banking information beyond that which was strictly
17 necessary to effectuate transfer or receipt of payments from or to his bank account; (c) would
18 collect, receive, or store any transaction-related banking information beyond the specific
19 transactions he triggered using the Venmo app; (d) would sell his banking data to Venmo; or
20 (e) would use or monetize his banking data in any way.

21 86. By logging into his bank account when prompted in the Venmo app, Mr. Cottle
22 intended only to prompt his bank to provide Venmo with access to his account for the limited
23 purposes of withdrawing funds for transfers he triggered in the Venmo account and depositing
24 funds for transfers other Venmo users made to him.

25 87. If Mr. Cottle had learned what he now knows about the existence and role of Plaid,
26 or the practices of Plaid in collecting, receiving, storing, selling, or using his banking data, he
27 would not have connected his bank account in the Venmo app the way he did.
28

1 88. Mr. Cottle is informed and believes that Plaid: (a) collected his private bank login
2 credentials; (b) accessed, downloaded, transferred, stored, enriched, and analyzed his private
3 banking information and data; (c) sold his private banking information to Venmo; and
4 (d) monetized his private banking data by performing analytics on it and using it to develop
5 value-added products for Plaid's customers. Mr. Cottle did not and does not consent to these
6 activities.

7 89. As a result of Plaid's actions, Mr. Cottle has suffered harm to his dignitary rights
8 and interests as a human being, and emotional distress, including anxiety, concern, and unease
9 about unauthorized parties accessing, storing, selling, and using his most private financial
10 information and intruding upon his private affairs and concerns. He also fears that he is at
11 increased risk of identity theft and fraud. He regularly monitors his credit, bank, and other
12 account statements for evidence of identity theft and fraud, and anticipates continuing to do so for
13 the foreseeable future.

14 90. Mr. Cottle's financial account at Wells Fargo was "linked" to and verified for use
15 with the Venmo app. Mr. Cottle has used Wells Fargo's password-protected interface with its
16 servers and systems to receive communications about his financial account, including without
17 limitation bank statements addressed to him and a listing of his recent account activity, as well as
18 messages, notifications, and other transfers of information.

19 91. In addition, Mr. Cottle has opened a bank account for his minor child. This
20 account is associated with Mr. Cottle's accounts and accessible with Mr. Cottle's Wells Fargo
21 username and password; thus, pursuant to the application of Plaid's policies, this minor
22 individual's account was accessed by Plaid repeatedly and without authorization.

23 92. Plaintiff **Frederick Schoeneman** signed up to use the Venmo app on or about July
24 15, 2016 via his mobile phone. When Mr. Schoeneman established his account with Venmo, he
25 did so for the purpose, consistent with the services offered by Venmo, of being able to send and
26 receive payments to or from friends, acquaintances, and other consumers.

27 93. Mr. Schoeneman does not recall specific details regarding the process of logging
28 into his bank account in the Venmo app so that he could send and receive money through the app.

1 He does not recall being prompted to read any privacy policy during the process of logging into
2 his bank account and does not recall having ever read any privacy policy from Venmo or Plaid
3 when he linked his bank account. He does not recall being sent any privacy policy after signing
4 up, or subsequently seeing any updates to a privacy policy related to his Venmo account or its
5 connection to his bank account.

6 94. At the time Mr. Schoeneman established his account with Venmo, he was not
7 aware of the existence or role of Plaid. When he was prompted in the Venmo app to log into his
8 bank account, he believed he was doing so through an official connection with his bank. He was
9 unaware that he was providing his login credentials to Plaid.

10 95. When Mr. Schoeneman was prompted in the Venmo app to log into his bank
11 account, he was not aware that Plaid: (a) would collect any of his banking information as part of
12 that process; (b) would collect, receive, or store any of his banking information beyond that which
13 was strictly necessary to effectuate transfer or receipt of payments from or to his bank account;
14 (c) would collect, receive, or store any transaction-related banking information beyond the
15 specific transactions he triggered using the Venmo app; (d) would sell his banking data to
16 Venmo; or (e) would use or monetize his banking data in any way.

17 96. By logging into his bank account when prompted in the Venmo app, Mr.
18 Schoeneman intended only to prompt his bank to provide Venmo with a connection to his account
19 for the limited purposes of withdrawing funds for transfers he triggered in the Venmo account and
20 depositing funds for transfers other Venmo users made to him.

21 97. If Mr. Schoeneman had learned what he now knows about the existence and role
22 of Plaid, or the practices of Plaid in collecting, receiving, storing, selling, or using his banking
23 data, he would not have connected his bank account in the Venmo app the way he did.

24 98. Since the time Mr. Schoeneman established his account with Venmo, he has used
25 the app sparingly.

26 99. Mr. Schoeneman is informed and believes that Plaid: (a) collected his private bank
27 login credentials; (b) accessed, downloaded, transferred, stored, enriched, and analyzed his
28 private banking information and data; (c) sold his private banking information to Venmo; and

1 (d) monetized his private banking data by performing analytics on it and using it to develop
2 value-added products for Plaid's customers. Mr. Schoeneman did not and does not consent to
3 these activities.

4 100. Mr. Schoeneman has suffered actual and concrete injury as a result of Plaid's
5 misconduct, including economic damages caused by the misappropriation of his sensitive
6 financial and personal data, harm to his dignitary rights and interests as a human being, as well as
7 emotional distress, including anxiety, concern, and unease about unauthorized parties accessing,
8 storing, selling, and using his most private financial information and intruding upon his private
9 affairs and concerns. He also is at increased risk of identity theft and fraud and now spends
10 approximately two hours each month monitoring his credit, bank, and other account statements
11 for evidence of identity theft and fraud. He anticipates continuing to do so for the foreseeable
12 future.

13 101. Mr. Schoeneman's financial account at Wells Fargo Bank was "linked" to and
14 verified for use with the Venmo app. Mr. Schoeneman has used Wells Fargo's password-
15 protected interface with its servers and systems to receive communications about his financial
16 account, including without limitation bank statements addressed to him and a listing of his recent
17 account activity, as well as messages, notifications, and other transfers of information.

18 **B. Injuries from Invasions of Privacy and Dignitary Violations**

19 102. Plaintiffs and Class members suffered a massive invasion of privacy and intrusion
20 upon their dignitary rights when Plaid, without their knowledge or consent, obtained access to
21 their personal financial accounts and stripped out all available data, including without limitation:
22 (a) their account numbers; (b) years of transactional data for every linked account (revealing what
23 they spent money on and where and when they spent it, including the name of the merchant and
24 transaction amount as well as the address and geolocation where each transaction occurred);
25 (c) account balances; (d) their detailed personal information including names, addresses, phone
26 numbers, and emails; (e) detailed investment information, including current holdings, value and
27 cost basis of investments, and investment transaction history; (f) information about annual salary
28 and income sources (*i.e.*, employment information); (g) detailed information about liabilities,

1 including payment histories, historical balances, and interest rates; and (h) bank account and other
2 identifying information about their minor children.⁷⁰ Plaintiffs and Class members reasonably
3 believed that this information was private and would not be accessible without their informed
4 consent. Each time that Plaid gathered, used, sold, transmitted, and stored this incredibly sensitive
5 and personal information, Plaid invaded Plaintiffs' and Class members' financial and other
6 privacy rights and violated their dignitary interests.

7 103. In addition, Plaintiffs and Class members suffered invasions of privacy when Plaid
8 collected, analyzed, sold, and used their medical-related personally identifiable information, in
9 violation of requirements under HIPAA. Examples of such information are transactional data
10 related to expenditures for doctors, hospitals, clinics and other health care facilities, as well as
11 expenditures for prescription drugs and other treatments. Examples also include data connected
12 with healthcare-related liabilities, such as medical payment plans or loans for elective surgeries.
13 Plaintiffs and Class members reasonably believed that this information was private. Each time
14 that Plaid gathered, used, sold, transmitted, and stored this information, Plaid invaded Plaintiffs'
15 and Class members' right to privacy.

16 104. These invasions represent an egregious violation of established social norms.
17 Plaid's conduct violates its acknowledged obligations under the existing regulatory scheme for
18 financial institutions and defies common law privacy protections as well as standard practice in
19 the financial industry. Consumers uniformly recognize the sensitivity of financial account
20 information and reasonably expect adequate disclosures and protections, even in the context of
21 sharing with financial applications with which, unlike Plaid, consumers *intentionally* interact to
22 obtain "traditional banking services," including personal financial management and budgeting
23 services.

24 105. The privacy, sensitivity, and appropriate safeguarding of confidential financial
25 information are material to consumers. This materiality is reflected in the various statutes that
26

27
28 ⁷⁰ See <https://plaid.com/docs/>;
<https://web.archive.org/web/20160319102824/https://plaid.com/docs/>.

1 enshrine these principles and the long history of the common law (put another way, privacy is
2 material as a matter of law), as well as through numerous other sources.

3 106. For example, the materiality of maintaining financial privacy was confirmed in a
4 2018 survey about fintech apps and financial data by The Clearing House (“TCH”), a banking
5 association and payments company owned by the largest commercial banks. While Plaid was not
6 addressed by the survey—unsurprisingly given consumers’ general unawareness of it—and while
7 many of the survey participants likely used apps for more involved purposes than the
8 Participating Apps (which exist largely to facilitate payments), the relevant conclusions include:

9 a. High levels of sensitivity about data access and privacy. Virtually all consumers
10 (a full 99%) expressed at least some concern about data privacy and data sharing, and indeed
11 more than two-thirds (67%) were very or extremely concerned.⁷¹

12 b. Low levels of consumer understanding. Notwithstanding this universal concern,
13 “[b]etween 62% and 81% of financial app users are not aware that the apps may access a range
14 of data types, from their email address to their bank account username and password. Between
15 81% and 86% of users are not fully aware that the apps may take actions such as sell their data to
16 third parties or retain access to information even when the app is deleted.”⁷²

17 c. Consumers would like controls over third party access and use of data. A full 96%
18 of respondents cared about how their data was accessed and, while some favored having their
19 primary bank control who had access to their information, most wanted control and the right to
20 provide explicit consent.⁷³

21 107. Again, this survey did not even purport to address the facts where, as here, a
22 company disguises itself as a trusted financial institution, and uses and profits from the
23 information it acquires. The TCH survey defined “fintech apps” broadly to include “desktop or
24

25 ⁷¹ See Aug. 2018 publication by The Clearing House: *Fintech Apps and Data Privacy: New*
26 *Insights from Consumer Research*, [https://www.theclearinghouse.org/payment-](https://www.theclearinghouse.org/payment-systems/articles/2018/10/~media/d025e3d1e5794a75a0144e835cd056b3.ashx)
27 [systems/articles/2018/10/~media/d025e3d1e5794a75a0144e835cd056b3.ashx](https://www.theclearinghouse.org/payment-systems/articles/2018/10/~media/d025e3d1e5794a75a0144e835cd056b3.ashx); see also The
28 Clearing House infographic, [https://www.theclearinghouse.org/payment-](https://www.theclearinghouse.org/payment-systems/articles/2018/10/~link.aspx?id=22B1B06FB2B143CAA2E9DE8634064E00&z=z)
[systems/articles/2018/10/~link.aspx?id=22B1B06FB2B143CAA2E9DE8634064E00&z=z](https://www.theclearinghouse.org/payment-systems/articles/2018/10/~link.aspx?id=22B1B06FB2B143CAA2E9DE8634064E00&z=z).

⁷² *Id.*

⁷³ *Id.* at 7.

1 mobile financial applications that provide **traditional banking services**, including personal
 2 financial management services, budgeting/saving services, investment services, advisory services
 3 and/or lending services.”⁷⁴ The results of the survey would have revealed even more sensitivity to
 4 privacy and disclosure issues if the focus were on fintech apps, like the Participating Apps, that
 5 have the more limited function of enabling payments. The survey results thus strongly underscore
 6 the materiality of Plaid’s omissions and concealment concerning Plaintiffs’ and Class members’
 7 financial privacy at issue here.

8 **C. Economic Damages**

9 108. Plaintiffs and Class members also suffered significant economic damages,
 10 including: (a) the loss of valuable indemnification rights; (b) the diminished value of important
 11 data protection rights they possessed when their sensitive information was secured in the banking
 12 environment; (c) the loss of control over valuable property; and (d) the heightened risk of identity
 13 theft and fraud.

14 **1. Loss of Valuable Indemnification Rights**

15 109. Plaintiffs and Class members suffered economic damages when Plaid deceptively
 16 acquired their bank login credentials and informed their financial institutions that they had
 17 provided Plaid with permission to gain access to all information available in their bank accounts;
 18 Plaid’s conduct destroyed valuable indemnity rights possessed by Plaintiffs and Class members.

19 110. These rights arise from Regulation E, codified at 12 C.F.R. § 1005, which provides
 20 a number of legal protections for consumers when their login credentials at financial institutions
 21 are used, unbeknownst to them, to conduct unauthorized electronic funds transfers. Among other
 22 protections, a consumer’s liability for an unauthorized transfer is typically limited to a maximum
 23 of either \$50 or \$500, depending upon how soon the bank was notified of the unauthorized
 24 transfer. 12 C.F.R. § 1005.6.

25 111. Regulation E defines an “[u]nauthorized electronic fund transfer” as “an electronic
 26 fund transfer from a consumer’s account initiated by a person other than the consumer without
 27

28

⁷⁴ *Id.* (emphasis added).

1 actual authority to initiate the transfer and from which the consumer receives no benefit.” 12
 2 C.F.R. § 1005.2(m).

3 112. Plaid’s conduct eliminates consumers’ rights under Regulation E because the
 4 provision of login credentials may be construed as a grant of “authority” to conduct funds
 5 transfers. Specifically, banks have taken the position that where a consumer provides login
 6 credentials to a third party and an unauthorized transfer is then initiated by either the third party
 7 or another outside source as a result of a breach of the third party, “the transfer would be
 8 considered authorized by the bank because the client had furnished an access device (*i.e.* login
 9 credentials) to the [third party], leaving the customer liable for such transfers.”⁷⁵

10 113. The American Bankers Association has taken the position that banks are not liable
 11 under Regulation E for unauthorized transactions made by data aggregators, such as Plaid, to
 12 whom the consumer has provided login credentials. As a result, according to the Association,
 13 “banks are not liable” for unauthorized transactions made via data aggregators like Plaid, and if
 14 the aggregators are “unable or unwilling to reimburse the consumer, the consumer suffers the
 15 loss.”⁷⁶ Chase’s CEO likewise stated that “[w]hen customers give out their bank passcode, they
 16 may not realize that if a rogue employee at an aggregator uses this passcode to steal money from
 17 the customer’s account, the customer, not the bank, is responsible for any loss.”⁷⁷

18 114. As recognized by the American Bankers Association, when Plaid collected
 19 Plaintiffs’ and Class members’ sensitive financial information, that information left the “secure
 20 bank environment, where it is accorded longstanding legal protections, and [was] released into the
 21 data services market where it is accorded no more special status than data created through a
 22 consumer’s use of a social media platform.”⁷⁸

23 ⁷⁵ See Feb. 21, 2017 Response by Consumer Bankers Association to CFPB RFI,
 24 <https://www.consumerbankers.com/sites/default/files/CFPB%20-%20Docket%20No%20-%202016-0048%20-%20RFI%20Consumer%20Access%20to%20Financial%20Records.pdf>.

25 ⁷⁶ See Feb. 21, 2017 Response by American Bankers Association to CFPB RFI,
 26 <https://buckleyfirm.com/sites/default/files/Buckley%20Sandler%20InfoBytes%20-%20American%20Bankers%20Association%202017.02.21%20Comment%20Letter%20to%20CFPB%27s%20RFI%20CFPB-2016-0048.pdf>.

27 ⁷⁷ See Apr. 6, 2016 Letter from JPMorgan Chase to shareholders,
 28 <https://www.jpmorganchase.com/corporate/annual-report/2015/>.

⁷⁸ See Feb. 21, 2017 Response by American Bankers Association to CFPB RFI,

1 115. Thus, when Plaid collects and uses consumers' bank login information and
2 purports to have consumers' consent to Plaid's extraction and subsequent uses and sale of their
3 data, Plaid removes valuable protections afforded to those consumers in the event of unauthorized
4 transfers. Plaid has deprived those consumers of rights to be indemnified and reimbursed for the
5 amount of such transfers over the limit (*e.g.*, a consumer's right to be indemnified for \$9,950 for
6 an unauthorized \$10,000 transaction that was reported the next day).

7 116. In recognition of the severe impact of this loss of protection for consumers as a
8 result of data aggregators' practices, in May 2018, three prominent aggregators submitted a new
9 proposed framework (the "Soda framework") for the industry to follow in lieu of new
10 government regulation. Included in the core principles of the Soda framework was the
11 requirement that "[t]he entity responsible for a consumer's financial loss must make the consumer
12 whole." As described in an *American Banker* article, the Soda framework "answers a long-held
13 question on liability in saying the entity responsible for a consumer's financial loss must make
14 that consumer whole. For loss occurring due to the actions of a data aggregator's clients, the
15 aggregator would be responsible to "reasonably establish that [its clients] have capacity, through
16 capital, insurance, or any other means, to make whole any consumers who suffer a financial loss
17 as a result of a breach."⁷⁹

18 117. Plaid, however, ensures that consumers' loss of valuable indemnification rights is
19 complete. In stark contrast to the guidelines in the Soda framework, Plaid makes no offer to
20 indemnify users of the Participating Apps for fraudulent activity on their financial accounts or
21 other fraud perpetrated with use of their login credentials.

22 118. As a result, even while Plaid has robbed consumers of the valuable protections
23 afforded them in the event of unauthorized transfers using their bank information, it
24

25 <https://buckleyfirm.com/sites/default/files/Buckley%20Sandler%20InfoBytes%20-%20American%20Bankers%20Association%202017.02.21%20Comment%20Letter%20to%20CFPB%27s%20RFI%20CFPB-2016-0048.pdf>.

27 ⁷⁹ See May 10, 2018 *American Banker* article, *Who's on the hook for a hack? Aggregators team*
28 *up on answer*, <https://www.americanbanker.com/news/envestnet-yodlee-quovo-byallaccounts-unveil-data-sharing-framework>.

1 simultaneously has attempted to shield itself from any liability for unauthorized transfers that
2 occur as a result of its activities.

3 **2. Diminished Value of Rights to Protection of Data**

4 119. Plaintiffs and Class members suffered additional economic damages through
5 diminished value of their rights to protection of their banking data.

6 120. Without their knowledge or consent, Plaid: (a) took their most sensitive financial
7 information out of their banks' trusted, secure environment; (b) sold it to the Participating Apps
8 without adequate controls over what such apps would do with it; and (c) stored the information
9 elsewhere for its own purposes, including without limitation for the purposes of "enriching" and
10 analyzing it.

11 121. As the American Bankers Association has recognized, when data aggregators such
12 as Plaid move data out of the secure banking environment, they deprive consumers of valuable
13 protections afforded by law when the data resides in that environment.⁸⁰

14 **3. Loss of Control Over Valuable Property**

15 122. Plaintiffs and Class members suffered loss of use and control to Plaid of their own
16 sensitive financial information, property which has value to them.

17 123. There can be no question that Plaintiffs' and Class members' sensitive financial
18 information is property that has value. As an initial matter, that information obviously has
19 significant *present financial value* because (a) Plaid has built a very successful business,
20 generating tens of millions of dollars annually, off of selling that information to companies like
21 the Participating Apps; and (b) Visa has agreed to pay \$5.3 billion for Plaid, based mainly upon
22 the value of that financial information.

23 124. For the same reasons, Plaid has established that a market exists for Plaintiffs' and
24 Class members' sensitive financial information. That financial information has significant *future*
25 *financial value* to Plaid as well, which is evident given the company's plans to pivot and focus on
26

27 ⁸⁰ See Feb. 21, 2017 Response by American Bankers Association to CFPB RFI,
28 <https://buckleyfirm.com/sites/default/files/Buckley%20Sandler%20InfoBytes%20-%20American%20Bankers%20Association%202017.02.21%20Comment%20Letter%20to%20CFPB%27s%20RFI%20CFPB-2016-0048.pdf>.

1 monetizing that information through analytics and value-added services it builds using that
 2 information. It also has significant *competitive value* to Plaid, providing the company with a moat
 3 to protect its position against would-be competitors.

4 125. Plaintiffs and Class members suffered harm when Plaid took their property, sold it,
 5 and put it to use for present and future monetization in other forms, for its own enrichment.

6 **4. Increased Risk of Identity Theft and Fraud**

7 126. In addition to removing valuable existing protections, Plaid's actions in removing
 8 Plaintiffs' and Class members' sensitive banking data from the secure banking environment also
 9 create huge additional risks for Plaintiffs:

10 [T]he sheer volume and value of the aggregated data make data
 11 aggregators a priority target for criminals, including identity
 12 thieves. . . . Through a single source, the criminal may gain access
 13 to the consumer's checking and savings accounts, retirement
 14 accounts, certificates of deposits, credit cards, brokerage accounts,
 15 and insurance products. . . . This rich reward for a single hack,
 either of an aggregated database of personally identifiable
 information or of a single consumer's multiple accounts, makes
 data aggregators an attractive target for criminals. They obtain the
 key not to just a single room, but the key ring with keys to all the
 rooms.⁸¹

16 127. Plaid knowingly magnified this risk by creating a single point of failure whereby
 17 all consumers' bank login credentials, personal information, and banking data could be accessed
 18 through a single attack.

19 128. These risks have created tangible, economic injury to Plaintiffs and Class
 20 members. One such risk is that someone at Plaid, Venmo, or one of their partner companies,
 21 vendors or contractors (*e.g.*, an outside software developer) will use Plaintiffs' and Class
 22 members' banking information to conduct unauthorized transactions, causing direct financial loss
 23 to them. Other risks include identity theft and fraud using Plaintiffs' and Class members' private
 24 banking information and data, which may result in long-term injuries related to compromised
 25 accounts, damaged credit ratings, inability to obtain credit, fraudulent tax filings, dissemination of
 26

27 ⁸¹ See Feb. 21, 2017 Response by American Bankers Association to CFPB RFI,
 28 <https://buckleyfirm.com/sites/default/files/Buckley%20Sandler%20InfoBytes%20-%20American%20Bankers%20Association%202017.02.21%20Comment%20Letter%20to%20CFPB%27s%20RFI%20CFPB-2016-0048.pdf>.

1 inaccurate or fraudulent medical information, and loss of employment opportunities. The integrity
2 of Plaintiffs' and Class members' bank accounts and the banking information and data therein has
3 been permanently diminished, and now they face an expanded and imminent risk of economic
4 harm from unauthorized transfers, identity theft, and fraud.

5 129. That Plaintiffs and Class members may not yet be aware that harm has occurred
6 increases rather than diminishes their risk because they cannot take specific action to prevent
7 harm. In addition, Plaintiffs and Class members face increased risk of predatory conduct by those
8 who obtain access to their personal information and data without their knowledge.

9 **VII. CHOICE OF LAW**

10 130. California's substantive laws may be constitutionally applied to the claims of
11 Plaintiffs and the Nationwide Class members under the Due Process Clause, 14th Amend., § 1,
12 and the Full Faith and Credit Clause, art. IV., § 1, of the U.S. Constitution.

13 131. California has a significant contact, or significant aggregation of contacts, to the
14 claims asserted by each Plaintiff, thereby creating state interests that ensure that the choice of
15 California state law to the common-law claims is not arbitrary or unfair. Plaid's headquarters and
16 principal place of business are in California. Plaid conducts substantial business in California, and
17 upon information and belief the scheme alleged in this Complaint originated and was
18 implemented in California. Class members' data is pulled, stored, and aggregated by Plaid in
19 California. California has a strong interest in regulating Plaid's conduct under its laws.

20 132. The application of California law to the proposed Nationwide Class members
21 (defined below) is also appropriate under California's choice of law rules, namely, the
22 governmental interest test California uses for choice-of-law questions. California's interest would
23 be the most impaired if its laws were not applied.

24 **VIII. TOLLING, CONCEALMENT, AND ESTOPPEL**

25 133. The statutes of limitation applicable to Plaintiffs' claims are tolled as a result of
26 Plaid's knowing and active concealment of its conduct alleged herein.

27 134. Among other things, Plaid made misleading statements in the Plaid software
28 incorporated in fintech apps and made misleading public statements (including in publications

1 and to various government agencies and regulators), while intentionally hiding its true actions and
2 knowingly permitting the fintech apps to make statements that were misleading and concealed the
3 true nature of Plaid's conduct and operation.

4 135. Moreover, Plaintiffs were ignorant of the information essential to pursue their
5 claims, without any fault or lack of diligence on their own part.

6 136. Furthermore, under the circumstances Plaid was under a duty to disclose the true
7 character, quality, and nature of its activities to Plaintiffs. Plaid therefore is estopped from relying
8 on any statute of limitations.

9 137. All applicable statutes of limitation also have been tolled by operation of the
10 discovery rule. Specifically, Plaintiffs and other Class members could not have learned through
11 the exercise of reasonable diligence of Plaid's conduct as alleged herein.

12 138. Plaid's fraudulent concealment and omissions are common to Plaintiffs and Class
13 members.

14 **IX. CLASS ACTION ALLEGATIONS**

15 139. Plaintiffs incorporate by reference all the foregoing allegations.

16 140. Plaintiffs bring this action on behalf of themselves and all others similarly situated
17 pursuant to Rule 23(b)(2) and 23(b)(3) of the Federal Rules of Civil Procedure.

18 141. Plaintiffs seek to represent the following Classes:

19 **Nationwide Class:** All natural persons in the United States whose
20 accounts at a financial institution were accessed by Plaid using
21 login credentials obtained through Plaid's software incorporated in
22 a mobile or web-based fintech app that enables payments (including
ACH payments) or other money transfers, including without
23 limitation users of Venmo, Square's Cash App, Coinbase, and
24 Stripe, from January 1, 2013 to the present.

25 **California Class:** All natural persons in California whose accounts
26 at a financial institution were accessed by Plaid using login
27 credentials obtained through Plaid's software incorporated in a
28 mobile or web-based fintech app that enables payments (including
ACH payments) or other money transfers, including without
limitation users of Venmo, Square's Cash App, Coinbase, and
Stripe, from January 1, 2013 to the present.

1 142. Excluded from the Classes are Plaid, its current employees, co-conspirators,
2 officers, directors, legal representatives, heirs, successors and wholly or partly owned subsidiaries
3 or affiliated companies; the undersigned counsel for Plaintiffs and their employees; and the Judge
4 and court staff to whom this case is assigned.

5 143. The Classes and their counsel satisfy the prerequisites of Federal Rule of Civil
6 Procedure 23(a) and 23(g) and the requirements of Rule 23(b)(3).

7 144. Numerosity and Ascertainability: Plaintiffs do not know the exact size of the
8 Classes or the identities of the Class members. Such information is known to Plaid. At minimum,
9 each Class has thousands or millions of members. Reports indicate that Plaid has accessed
10 approximately 200 million United States financial accounts. Venmo had over 52 million active
11 accounts at the end of 2019.⁸² Coinbase reportedly has more than 30 million users.⁸³ Square's
12 Cash App reportedly has more than 24 million monthly active users.⁸⁴ Thus, the number of
13 members in each Class is so numerous that joinder of all Class members is impracticable. The
14 names, addresses, and phone numbers of Class members are identifiable through documents
15 maintained by Plaid, and also available from the records of third parties such as Class members'
16 financial institutions and the Participating Apps.

17 145. Commonality and Predominance: The action involves numerous common
18 questions of law and fact that predominate over any question solely affecting individual Class
19 members. These common questions for Class members' claims include, but are not limited to, the
20 following:

- 21 (1) Whether Plaid omitted or concealed material facts from Plaintiffs
22 and Class members;
- 23 (2) Whether Plaid owes a duty to Plaintiffs and Class members to
24 disclose material facts;
- 25 (3) Whether Plaid gave effective notice of its privacy policy under an

26 ⁸² See <https://investor.paypal-corp.com/static-files/0b7b0dda-a4ee-4763-9eee-76c01be0622c>.

27 ⁸³ See <https://www.coinbase.com/about>.

28 ⁸⁴ See <https://www.businessinsider.com/squares-cash-app-reached-24-million-users-and-monetization-surge-2020-2>.

- 1 objectively reasonable consumer standard;
- 2 (4) Whether Plaid’s privacy policy discloses Plaid’s conduct;
- 3 (5) Whether credentials obtained through Plaid’s Managed OAuth
- 4 procedure were obtained with Plaintiffs’ and Class members’
- 5 informed consent;
- 6 (6) Whether Plaid’s use of Plaintiffs’ and Class members’ banking
- 7 credentials obtained through Plaid’s Managed OAuth procedure to
- 8 access Plaintiffs’ and Class members’ financial institution accounts
- 9 was done with Plaintiffs’ and Class members’ informed consent;
- 10 (7) Whether Plaid obtained broad financial data from Class members’
- 11 bank accounts;
- 12 (8) Whether Plaid’s acts and practices complained of herein amount to
- 13 egregious breaches of social norms;
- 14 (9) Whether Plaid’s conduct described herein violates Plaintiffs’ and
- 15 Class members’ interest in precluding the dissemination or misuse
- 16 of sensitive and confidential information (“informational
- 17 privacy”);
- 18 (10) Whether Plaid’s conduct described herein violates Plaintiffs’ and
- 19 Class members’ interest in making intimate personal decisions or
- 20 conducting personal activities without observation, intrusion, or
- 21 interference (“autonomy privacy”);
- 22 (11) Whether the computer systems operated by Plaintiffs’ and Class
- 23 members’ financial institutions are “protected computers” or
- 24 “computers of financial institutions” under the CFAA;
- 25 (12) Whether Plaid intentionally accessed protected computer systems
- 26 in violation of the CFAA;
- 27 (13) Whether Plaid improperly obtained and disclosed Plaintiffs’ and
- 28 Class members’ financial information without authorization or in

- 1 excess of any authorization;
- 2 (14) Whether Plaid knowingly trafficked in access tokens or similar
- 3 information so the Participating Apps could access Plaintiffs' and
- 4 Class members' private data from their financial institutions;
- 5 (15) Whether Plaid's conduct violated the Stored Communications Act,
- 6 18 U.S.C. § 2701, *et seq.*;
- 7 (16) Whether profits obtained by Plaid through sale of information or
- 8 sale of access to information obtained from Plaintiffs' and Class
- 9 members' financial accounts were unjustly obtained by Plaid and
- 10 should be disgorged;
- 11 (17) Whether any profits or other value obtained by Plaid through
- 12 analysis, enrichment, and other use of information from Plaintiffs'
- 13 and Class members' financial accounts were unjustly obtained by
- 14 Plaid and should be disgorged;
- 15 (18) Whether declaratory relief and an injunction should be granted;
- 16 (19) Whether Plaid's conduct violated the California Constitution;
- 17 (20) Whether Plaid, through its Managed OAuth process, induced
- 18 California Class members to provide "identifying information"
- 19 within the meaning of the California Anti-Phishing Act by
- 20 representing itself to be a business without the authority or
- 21 approval of the business;
- 22 (21) Whether Plaintiffs and Class members are "adversely affected"
- 23 within the meaning of the California Anti-Phishing Act by the
- 24 collection of their financial institution login credentials and
- 25 identifying information by Plaid or by Plaid's subsequent use and
- 26 sale of such information;
- 27 (22) Whether Plaid's conduct was an unlawful, unfair, or fraudulent
- 28 business practice under Cal. Bus. & Prof. Code § 17200, *et seq.*;

1 (23) Whether Plaintiffs and Class members are entitled to compensation
2 resulting from the loss caused by Plaid of a right to indemnity by
3 their financial institutions in the event of fraudulent conduct on
4 their accounts;

5 (24) Whether Plaintiffs and Class members are entitled to compensation
6 resulting from the heightened risk of identity theft and fraud
7 caused by Plaid's transfer of their identifying information from
8 secure financial institutions to itself and to other parties; and

9 (25) Whether Plaid's conduct alleged herein was knowing, willful, and
10 intentional.

11 146. Plaid engaged in a common course of conduct giving rise to the legal rights sought
12 to be enforced by this action. Furthermore, similar or identical questions of statutory and common
13 law, as well as similar or identical injuries, are involved. Individual questions, if any, pale in
14 comparison to the numerous common questions that predominate in this action.

15 147. Typicality: Plaintiffs' claims are typical of the other Class members' claims
16 because all Class members were comparably injured through Plaid's substantially uniform
17 misconduct as described above. The Plaintiffs representing the Classes are advancing the same
18 claims and legal theories on behalf of themselves and all other members of the Classes that they
19 represent, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and
20 Class members arise from the same operative facts and are based upon the same legal theories.

21 148. Adequacy: Plaintiffs are adequate Class representatives because their interests do
22 not conflict with the interests of the other members of the Class they seek to represent; Plaintiffs
23 have retained counsel competent and experienced in complex class action litigation, and Plaintiffs
24 intend to prosecute this action vigorously. The interests of the Classes will be fairly and
25 adequately protected by Plaintiffs and their counsel.

26 149. Superiority: A class action is superior to any other available means for the fair and
27 efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered
28 in the management of this class action. The damages and other harm suffered by Plaintiffs and

1 Class members are relatively small compared to the burden and expense that would be required to
 2 individually litigate their claims against Plaid, so it would be virtually impossible for Class
 3 members individually to seek redress for Plaid’s wrongful conduct. Even if Class members could
 4 afford individual litigation, the court system could not. Individualized litigation creates a potential
 5 for inconsistent or contradictory judgments, and increases the delay and expense to all parties and
 6 the court system. By contrast, the class action device presents far fewer management difficulties,
 7 and provides the benefits of single adjudication, economy of scale, and comprehensive
 8 supervision by a single court.

9 150. Class certification under Rule 23(b)(2) is also warranted for purposes of injunctive
 10 and declaratory relief because Plaid has acted or refused to act on grounds generally applicable to
 11 the Classes, so that final injunctive and declaratory relief are appropriate with respect to the
 12 Classes as a whole.

13 **X. CLAIMS FOR RELIEF**

14 **FIRST CAUSE OF ACTION**

15 **Invasion of Privacy—Intrusion into Private Affairs**

16 151. Plaintiffs incorporate the substantive allegations contained in all prior and
 17 succeeding paragraphs as if fully set forth herein. These include the choice of law discussion.
 18 Specifically, California law on intrusion upon seclusion is applicable nationwide because there is
 19 no conflict of law between the law in California and in states that have expressly or, via
 20 jurisprudence, impliedly adopted the Restatement (Second) of Torts, § 652B. Alternatively, no
 21 state has a greater interest than California in applying its laws.

22 152. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class
 23 (referred to in this claim as “the Class”).

24 153. Plaintiffs and Class members have a reasonable expectation of privacy in the
 25 personal information and banking data maintained at their banks. The reasonableness of this
 26 expectation is reflected in longstanding custom and practice, security measures intended to
 27 prevent unauthorized access to banking account information, state, federal, and international laws
 28 protecting a right to financial privacy, and the privacy policies and other assurances of protection

1 by applications that use Plaid discussed herein, among other indicia. Plaintiffs and Class members
2 reasonably expected that their login credentials, account numbers, balances, transaction history,
3 and other information was private and secure within the banks at which they maintain accounts.
4 They reasonably expected that their information and data (a) would be protected and secured
5 against access by unauthorized parties; (b) would not be obtained by unauthorized parties;
6 (c) would not be transmitted or stored outside of the secure bank environment; and (d) would not
7 be sold or used without their knowledge or permission.

8 154. Plaid intentionally intruded upon Plaintiffs' and Class members' private affairs
9 and concerns by improperly accessing, downloading, transferring, selling, storing and using their
10 private banking information and data.

11 155. The manner in which Plaid obtained access to Plaintiffs' and Class members'
12 banking login credentials, account numbers, balances, transaction history, and other information
13 stored by their banks was highly offensive to Plaintiffs and would be highly offensive to a
14 reasonable person. Each of (a) obtaining login credentials through covert means including by
15 falsely suggesting, through use of design, overt and implied statements, and context, that
16 consumers were communicating directly with their banks when they entered login credentials;
17 (b) retaining login credentials for purposes other than verifying information about a consumer's
18 bank account that was required for use of the relevant payment application; (c) using the illicitly-
19 obtained login credentials to access historical banking information not required for use of the
20 relevant payment application; (d) retaining, analyzing, and profiting from such information;
21 (e) using the illicitly-obtained login credentials to access banking information after the date on
22 which such credentials were initially provided; (f) retaining, analyzing, and profiting from such
23 information; and (g) failing to disclose such conduct, constitute egregious violations of social
24 norms.

25 156. Plaid's intrusions upon Plaintiffs' and Class members' private affairs and concerns
26 would be highly offensive to a reasonable person, especially considering (a) the highly sensitive
27 and personal nature of Plaintiffs' and Class members' banking information and data; (b) the
28 extensive scope of data obtained by Plaid, including years of historical transactional data;

1 (c) Plaid's intent to profit from Plaintiffs' and Class members' data by selling it outright and
2 using it to develop further products and services; (d) Plaid's use of subterfuge to intrude into
3 Plaintiffs' and Class members' banks' secure environments for the purpose of collecting their
4 data; (e) the surreptitious and unseen nature of Plaid's data collection with respect to consumers,
5 and (f) Plaid's failure to obtain consumers' consent to its conduct. Plaid's intrusions were
6 substantial, and constituted an egregious breach of social norms.

7 157. Plaintiffs and Class members did not consent to Plaid's intrusions upon their
8 private affairs and concerns.

9 158. Plaid's conduct described herein violates Plaintiffs' and Class members' interests
10 in precluding the dissemination or misuse of sensitive and confidential information (*i.e.*, their
11 informational privacy rights), including without limitation the privacy of information about their
12 income, generosity, charitable giving, retirement contributions, healthcare costs, healthcare
13 treatment, shopping habits, dining habits, entertainment habits, saving and spending habits, credit
14 repayment habits, locations, identity information including contact data, familial information, and
15 other information available to their financial institutions, as well as the terms of any loans and
16 other financial affairs.

17 159. Plaid's conduct described herein violates Plaintiffs' and Class members' interests
18 in making intimate personal decisions or conducting personal activities without observation,
19 intrusion, or interference (*i.e.*, their autonomy privacy rights) because, without limitation, Plaid
20 accesses the information described in the preceding paragraph multiple times per day, at a
21 minimum every 4-6 hours, and analyzes the private information for its own undisclosed purposes
22 including, *inter alia*, to generate invasive profiles of Plaintiffs' and Class members' incomes,
23 debts, relationships, and personal lives.

24 160. Plaintiffs and Class members suffered actual and concrete injury as a result of
25 Plaid's intrusions upon their private affairs and concerns. Plaintiffs and Class members are
26 entitled to appropriate relief, including damages to compensate Plaintiffs and Class members for
27 the harm to their privacy interests, loss of valuable rights and protections, heightened risk of
28 future invasions of privacy, and the mental and emotional distress and harm to human dignity

1 interests caused by Plaid’s invasions, as well as disgorgement of profits made by Plaid as a result
2 of its intrusions upon Plaintiffs’ and Class members’ private affairs and concerns.

3 161. Plaintiffs and Class members also seek punitive damages because Plaid’s
4 actions—which were malicious, oppressive, and willful—were calculated to injure Plaintiffs and
5 Class members and made in conscious disregard of Plaintiffs’ and Class members’ rights.
6 Punitive damages are warranted to deter Plaid from engaging in future misconduct.

7 **SECOND CAUSE OF ACTION**

8 **Violation of the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030**

9 162. Plaintiffs incorporate the substantive allegations contained in all prior and
10 succeeding paragraphs as if fully set forth herein.

11 163. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class
12 (referred to in this claim as “the Class”).

13 164. The CFAA prohibits unauthorized access to computers and the private financial
14 data stored on those computers, as well as trafficking in password information for computers.
15 Through its actions described herein, Plaid has committed multiple violations of the CFAA.

16 **A. Violations of 18 U.S.C. § 1030(a)(2)**

17 165. Plaid intentionally accessed a computer under 18 U.S.C. §§ 1030(a)(2) &
18 1030(e)(1) by intentionally accessing Plaintiffs’ and Class members’ personal financial accounts,
19 and specifically the financial institutions’ computer systems, data storage facilities, or
20 communications facilities.

21 166. Plaintiffs’ and Class members’ banks’ computer systems constitute both protected
22 computers and computers of financial institutions under 18 U.S.C. §§ 1030(a)(2)(C) &
23 1030(e)(2)(A)-(B) because (i) they were exclusively for the use of a financial institution, (ii) they
24 were used by a financial institution, and Plaid’s conduct affected the banks’ use of their systems,
25 and (iii) they were used in or affected interstate or foreign commerce or communication.

26 167. Plaid violated 18 U.S.C. § 1030(a)(2)(A) when it intentionally accessed Plaintiffs’
27 and Class members’ banks’ computer systems without authorization, and thereby obtained
28 information contained in a financial record of a financial institution, including all of the private

1 data Plaid collected from Plaintiffs' and Class members' banking records. Plaintiffs and Class
2 members did not grant express or implied authority for Plaid to access their banks' computer
3 systems.

4 168. Alternatively, Plaid violated 18 U.S.C. § 1030(a)(2)(A) when it intentionally
5 accessed Plaintiffs' and Class members' banks' computer systems and such access exceeded
6 authorization, and thereby obtained information contained in a financial record of a financial
7 institution. Plaintiffs and Class members did not grant express or implied authority for Plaid to
8 access any data in their banks' computer systems beyond that which was strictly necessary to
9 facilitate transactions Plaintiffs and Class members conducted in the Participating Apps. Plaid
10 exceeded authorized access under 18 U.S.C. § 1030(e)(6) by using its access to the banks'
11 computer systems to obtain information it was not entitled to obtain, in the form of data that was
12 not strictly necessary to facilitate Participating App transactions, including Plaintiffs' and Class
13 members' detailed banking transaction histories.

14 169. Plaid violated 18 U.S.C. § 1030(a)(2)(C) when it intentionally accessed Plaintiffs'
15 and Class members' banks' computer systems without authorization, and thereby obtained both
16 information in a financial record of a financial institution and information from a protected
17 computer, including all of the private data Plaid collected from Plaintiffs' and Class members'
18 banking records. Plaintiffs and Class members did not grant express or implied authority for Plaid
19 to access their banks' computer systems.

20 170. Alternatively, Plaid violated 18 U.S.C. § 1030(a)(2)(C) when it intentionally
21 accessed Plaintiffs' and Class members' banks' computer systems and such access exceeded
22 authorization, and thereby obtained both information in a financial record of a financial institution
23 and information from a protected computer. Plaintiffs and Class members did not grant express or
24 implied authority for Plaid to access any data in their banks' computer systems beyond that which
25 was strictly necessary to facilitate transactions Plaintiffs conducted in the Participating Apps.
26 Plaid exceeded authorized access under 18 U.S.C. § 1030(e)(6) by using its access to the banks'
27 computer systems to obtain information it was not entitled to obtain, in the form of data that was
28

1 not strictly necessary to facilitate Participating App transactions, including Plaintiffs' and Class
2 members' detailed banking transaction histories.

3 **B. Violations of 18 U.S.C. § 1030(a)(4)**

4 171. Plaid knowingly accessed a protected computer under 18 U.S.C. §§ 1030(a)(4) &
5 1030(e)(1)-(2) by knowingly accessing Plaintiffs' and Class members' banks' computer systems,
6 data storage facilities, or communications facilities.

7 172. Plaid acted with intent to defraud in accessing a protected computer under 18
8 U.S.C. §§ 1030(a)(4) & 1030(e)(1)-(2) by accessing Plaintiffs' and Class members' banks'
9 computer systems, data storage facilities, or communications facilities with the intent to collect
10 banking data to which it was not entitled and which it intended to sell and use without authority.

11 173. Plaid violated 18 U.S.C. § 1030(a)(4) when it intentionally accessed Plaintiffs'
12 banks' computer systems without authorization, and thereby furthered its intended fraud and
13 obtained a thing of value, including all of the private data Plaid collected from Plaintiffs' and
14 Class members' banking records, as well as the use of the banks' computer system. Plaintiffs and
15 Class members did not grant express or implied authority for Plaid to access their banks'
16 computer systems.

17 174. Alternatively, Plaid violated 18 U.S.C. § 1030(a)(4) when it intentionally accessed
18 Plaintiffs' and Class members' banks' computer systems and such access exceeded authorization,
19 and thereby furthered its intended fraud and obtained a thing of value, including all of the private
20 data Plaid collected from Plaintiffs' and Class members' banking records, as well as the use of the
21 banks' computer systems. Plaintiffs and Class members did not grant express or implied authority
22 for Plaid to access any data in their banks' computer systems beyond that which was strictly
23 necessary to facilitate transactions Plaintiffs and Class members conducted in the Participating
24 Apps. Plaid exceeded authorized access under 18 U.S.C. § 1030(e)(6) by using its access to the
25 banks' computer systems to obtain information it was not entitled to obtain, in the form of data
26 that was not strictly necessary to facilitate Participating App transactions, including Plaintiffs'
27 and Class members' detailed banking transaction histories.

28

1 **C. Violations of 18 U.S.C. § 1030(a)(5)(A)**

2 175. Plaid knowingly caused the transmission of a program, information, code, or
3 command under 18 U.S.C. § 1030(a)(5)(A) by (1) knowingly transmitting Plaintiffs’ and Class
4 members’ bank login information to access their banks’ computer systems, data storage facilities,
5 or communications facilities; and (2) knowingly transmitting its software to the Participating
6 Apps for incorporation into their apps so that Plaid could collect Plaintiffs’ and Class members’
7 bank login information.

8 176. Plaid violated 18 U.S.C. § 1030(a)(5)(A) when it knowingly caused the
9 transmission of a program, information, code, or command, and as a result, intentionally caused
10 damage without authorization to the banks’ computer systems and Plaintiffs’ and Class members’
11 data contained therein, as well as to Plaintiffs’ and Class members’ smartphones and their data
12 contained therein.

13 177. Plaid caused Plaintiffs and Class members damage under 18 U.S.C.
14 §§ 1030(a)(5)(A) and 1030(e)(8), including in the following ways:

15 a. Plaid removed Plaintiffs’ and Class members’ banking data from the secure
16 banking environment and placed it in an environment where it was subject to increased risk of
17 loss or theft, including by selling or transferring it to the Participating Apps and by storing it for
18 its own use. Plaid thereby destroyed the valuable indemnification rights Plaintiffs and Class
19 members had against loss when that data was in the bank environment. Plaid also thereby
20 removed valuable additional protections (including regulatory protections) Plaintiffs’ and Class
21 members’ data had when that data was in the bank environment. As a result, the integrity of
22 Plaintiffs’ and Class members’ data has been irreparably impaired.

23 b. Plaid used its software to obtain an open connection to Plaintiffs’ and Class
24 members’ bank accounts so that it could control access to, and take information from, Plaintiffs’
25 banks’ computer systems. Plaid thereby impaired the integrity of both the banks’ computer
26 systems and Plaintiffs’ and Class members’ data contained therein.

27 c. Plaid impaired the integrity of Plaintiffs’ and Class members’ smartphones by
28 installing software within the Participating Apps that captured their sensitive bank login data for

1 use in logging into Plaintiffs' and Class members' bank accounts. Plaid thereby impaired the
2 integrity of both Plaintiffs' and Class members' smartphones and their data contained therein.

3 d. Plaid accessed Plaintiffs' and Class members' bank' computer systems, copied
4 their banking data, sold it to the Participating Apps, and used it for its own purposes. Plaid
5 thereby impaired the integrity of both the banks' computer systems and Plaintiffs' and Class
6 members' data contained therein.

7 **D. Violations of 18 U.S.C. § 1030(a)(5)(B)**

8 178. Plaid intentionally accessed a protected computer under 18 U.S.C.
9 §§ 1030(a)(5)(B) & 1030(e)(1)-(2) by (1) intentionally accessing Plaintiff's and Class members'
10 banks' computer systems, data storage facilities, or communications facilities; and
11 (2) intentionally accessing Plaintiffs' and Class members' smartphones by incorporating its
12 software into the Participating Apps so that Plaid could collect Plaintiffs' and Class members'
13 bank login information.

14 179. Plaid violated 18 U.S.C. § 1030(a)(5)(B) when it intentionally accessed a protected
15 computer without authorization, and thereby at least recklessly caused damage to the banks'
16 computer systems and Plaintiffs' and Class members' data contained therein, as well as to
17 Plaintiffs' and Class members' smartphones and their data contained therein. Plaintiffs and Class
18 members did not grant express or implied authority for Plaid to access either their banks'
19 computer systems or their smartphones.

20 180. Plaid caused Plaintiffs and Class members damage under 18 U.S.C.
21 §§ 1030(a)(5)(A) and 1030(e)(8), including in the following ways:

22 a. Plaid removed Plaintiffs' and Class members' banking data from the secure
23 banking environment and placed it in an environment where it was subject to increased risk of
24 loss or theft, including by selling or transferring it to the Participating Apps and by storing it for
25 its own use. Plaid thereby destroyed the valuable indemnification rights Plaintiffs and Class
26 members had against loss when that data was in the bank environment. Plaid also thereby
27 removed valuable additional protections (including regulatory protections) Plaintiffs' and Class
28

1 members' data had when that data was in the bank environment. As a result, the integrity of
2 Plaintiffs' and Class members' data has been irreparably impaired.

3 b. Plaid used its software to obtain an open connection to Plaintiffs' and Class
4 members' bank accounts so that it could control access to, and steal information from, Plaintiffs'
5 and Class members' banks' computer systems. Plaid thereby impaired the integrity of both the
6 banks' computer systems and Plaintiffs' and Class members' data contained therein.

7 c. Plaid impaired the integrity of Plaintiffs' and Class members' smartphones by
8 installing software within the Participating Apps that captured their sensitive bank login data for
9 use in logging into Plaintiffs' and Class members' bank accounts. Plaid thereby impaired the
10 integrity of both Plaintiffs' and Class members' smartphones and their data contained therein.

11 d. Plaid accessed Plaintiffs' and Class members' banks' computer systems, copied
12 Plaintiffs' and Class members' banking data, sold it to the Participating Apps, and used it for its
13 own purposes. Plaid thereby impaired the integrity of both the banks' computer systems and
14 Plaintiffs' and Class members' data contained therein.

15 **E. Violations of 18 U.S.C. § 1030(a)(5)(C)**

16 181. Plaid intentionally accessed a protected computer under 18 U.S.C.
17 §§ 1030(a)(5)(C) & 1030(e)(1)-(2) by (1) intentionally accessing Plaintiffs' and Class members'
18 banks' computer systems, data storage facilities, or communications facilities; and
19 (2) intentionally accessing Plaintiffs' and Class members' smartphones by incorporating its
20 software into the Participating Apps so that Plaid could collect Plaintiffs' and Class members'
21 bank login information.

22 182. Plaid violated 18 U.S.C. § 1030(a)(5)(C) when it intentionally accessed a protected
23 computer without authorization, and thereby caused both damage and loss to the banks' computer
24 systems and Plaintiffs' and Class members' data contained therein, as well as to Plaintiffs' and
25 Class members' smartphones and their data contained therein. Plaintiffs and Class members did
26 not grant express or implied authority for Plaid to access either their banks' computer systems or
27 their smartphones.

28

1 183. Plaid caused Plaintiffs and Class members damage under 18 U.S.C.
2 §§ 1030(a)(5)(A) and 1030(e)(8), including in the following ways:

3 a. Plaid removed Plaintiffs' and Class members' banking data from the secure
4 banking environment and placed it in an environment where it was subject to increased risk of
5 loss or theft, including by selling or transferring it to the Participating Apps and by storing it for
6 its own use. Plaid thereby destroyed the valuable indemnification rights Plaintiffs and Class
7 members had against loss when that data was in the bank environment. Plaid also thereby
8 removed valuable additional protections (including regulatory protections) Plaintiffs' and Class
9 members' data had when that data was in the bank environment. As a result, the integrity of
10 Plaintiffs' and Class members' data has been irreparably impaired.

11 b. Plaid used its software to obtain an open connection to Plaintiffs' and Class
12 members' bank accounts so that it could control access to, and steal information from, Plaintiffs'
13 and Class members' banks' computer systems. Plaid thereby impaired the integrity of both the
14 banks' computer systems and Plaintiffs' and Class members' data contained therein.

15 c. Plaid impaired the integrity of Plaintiffs' and Class members' smartphones by
16 installing software within the Participating Apps that captured their sensitive bank login data for
17 use in logging into Plaintiffs' and Class members' bank accounts. Plaid thereby impaired the
18 integrity of both Plaintiffs' and Class members' smartphones and their data contained therein.

19 d. Plaid accessed Plaintiffs' and Class members' bank' computer systems, copied
20 Plaintiffs' and Class members' banking data, sold it to the Participating Apps, and used it for its
21 own purposes. Plaid thereby impaired the integrity of both the banks' computer systems and
22 Plaintiffs' and Class members' data contained therein

23 184. Plaid caused Plaintiffs and Class members loss under 18 U.S.C. §§ 1030(a)(5)(A)
24 and 1030(e)(11), including in the following ways:

25 a. Plaid removed Plaintiffs' and Class members' banking data from the secure
26 banking environment, selling or transferring it to the Participating Apps and storing it for its own
27 use. Plaid thereby (1) destroyed the valuable indemnification rights Plaintiffs and Class members
28 had against loss when that data was in the bank environment; and (2) removed valuable

1 additional protections (including regulatory protections) Plaintiffs and Class members had when
2 that data was in the bank environment.

3 b. Plaid misappropriated Plaintiffs' and Class members' valuable banking data, sold
4 it, and stored and used it for its own purposes.

5 **F. Violations of 18 U.S.C. § 1030(a)(6)**

6 185. Plaid knowingly trafficked in passwords or similar information through which a
7 computer may be accessed without authorization under 18 U.S.C. §§ 1030(a)(6), 1030(e)(1), and
8 1029(e)(5) by knowingly obtaining control of access tokens or similar information from
9 Plaintiffs' and Class members' financial institutions through which the institutions' computer
10 systems could be accessed without authorization, with the intent to transfer such access tokens or
11 similar information to the Participating Apps so the Participating Apps could access Plaintiffs'
12 and Class members' private data from the institutions, including Plaintiffs' and Class members'
13 detailed banking transaction histories.

14 186. Alternatively, Plaid knowingly trafficked in passwords or similar information
15 through which a computer may be accessed without authorization under 18 U.S.C. §§ 1030(a)(6),
16 1030(e)(1), and 1029(e)(5) by knowingly transferring to the Participating Apps access tokens or
17 similar information from Plaintiffs' and Class members' banks through which the banks'
18 computer systems could be accessed without authorization using Plaid's software, so that those
19 entities so could use such access tokens or similar information to access Plaintiffs' and Class
20 members' private data from the banks, including Plaintiffs' and Class members' detailed banking
21 transaction histories.

22 187. Plaid acted with intent to defraud in trafficking the above-described passwords or
23 similar information under 18 U.S.C. §§ 1030(a)(6) & 1029(e)(5) by obtaining control of access
24 tokens or similar information and transferring such access tokens or similar information to the
25 Participating Apps with the intent that those entities would use such access tokens or similar
26 information to collect banking data to which they were not entitled, and that Plaid would be able
27 to charge the Participating Apps for the information or access.
28

1 188. Plaid’s trafficking activities affected interstate or foreign commerce under 18
2 U.S.C. § 1030(a)(6).

3 **G. Plaintiffs’ Right to Recover Damages**

4 189. As alleged above, Plaintiffs and Class members have suffered damage or loss by
5 reason of Plaid’s violations of the CFAA and are therefore entitled to recover compensatory
6 damages, as well as injunctive or other equitable relief as prayed for below, all pursuant to 18
7 U.S.C. § 1030(g). Plaid’s conduct has caused Plaintiffs and Class members losses in an amount
8 exceeding \$5,000 during a one-year period as required under 18 U.S.C. §§ 1030(g) and
9 1030(c)(4)(i)(I).

10 190. Plaintiffs bring this cause of action within two years of the date of the discovery of
11 their damages under 18 U.S.C. § 1030(g).

12 **THIRD CAUSE OF ACTION**

13 **Violation of the Stored Communications Act (“SCA”), 18 U.S.C. § 2701**

14 191. Plaintiffs incorporate the substantive allegations contained in all prior and
15 succeeding paragraphs as if fully set forth herein.

16 192. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class
17 (referred to in this claim as “the Class”).

18 193. The Stored Communications Act prohibits a person from intentionally accessing
19 without (or in excess of) authorization a facility through which an electronic communications
20 service is provided and thereby obtaining an electronic communication while it is in “electronic
21 storage.”

22 194. Each financial institution linked or verified for use with an Participating App, or
23 each such institution’s systems and servers, is a facility, which provides its users with the ability
24 to send and receive electronic communications, including, *inter alia*, images, data, queries,
25 messages, notifications, statements, forms, updates, and intelligence regarding the financial
26 institutions and their policies and promotions, as well as about customers’ individual accounts
27 and activities, among others. 18 U.S.C. §§ 2701(a)(1); 2711(1), 2510(15) & 2510(12). Financial
28 institutions communicate information about account holders’ financial affairs, including *inter alia*

1 account balances, historical transactions, pending transactions, withdrawals, deposits, transfers,
2 outgoing wires, loan terms, and interest rates through the electronic interface provided by
3 financial institutions for access via web browsers and the institutions' mobile apps.

4 195. The SCA defines "electronic storage" as "any temporary, intermediate storage of a
5 wire or electronic communication incidental to the electronic transmission thereof; and any
6 storage of such communication by an electronic communication service for purposes of backup
7 protection of such communication." Plaintiffs' and Class members' financial institution store the
8 communications alleged herein in their respective systems and databases and on their respective
9 servers.

10 196. For purposes of this cause of action only, the communications at issue exclude any
11 electronic funds transfer information stored by a financial institution in a communications system
12 used for the electronic storage and transfer of funds.

13 197. The communications at issue in this cause of action were in electronic storage
14 within the meaning of 18 U.S.C. § 2510(17) in that they were stored, among other reasons, for
15 purposes of backup protection of such electronic communications. Financial institutions
16 necessarily store historical communications regarding a customer's past banking activities,
17 historical direct messages, and other communications so that they may be accessed by consumers,
18 including Plaintiffs and Class members (*e.g.*, for tax purposes, to confirm that an authorized
19 payment was delivered, or to check on the status of a check).

20 198. Plaid's conduct in accessing these facilities and the communications stored
21 thereon, was intentional.

22 199. Plaid violated 18 U.S.C. § 2701(a)(1) when it intentionally accessed Plaintiffs' and
23 Class members' financial institutions and their systems and databases without authorization, and
24 thereby obtained access to the contents of Plaintiffs' and Class members' electronic
25 communications while those communications were in electronic storage on such systems. Plaid's
26 access to the banks' computer systems was not authorized by Plaintiffs or the financial
27 institutions.
28

1 provided by Plaid’s fintech clients to Plaintiffs and Class members, such as that their credentials
2 would “never be made accessible” to the Participating Apps and that their credentials were
3 “Secure”; and concealing that Plaid collects all available banking data from all available accounts
4 after it has accessed a consumer’s original, primary account.

5 213. Plaid was enriched when it utilized fraudulently obtained financial institution login
6 credentials to access, collect, store, aggregate, use, and sell—to the Participating Apps—years’
7 worth of Plaintiffs’ and Class members’ private banking records and transaction data. Plaid has
8 derived profits and other tangible benefits from this collection of data, without which Plaid could
9 not have grown its business, sold its platform to various and multiple developers, and developed
10 other apps. Furthermore, Plaid has directly and substantially profited from its use, storage,
11 aggregation, and sale of Plaintiffs’ and Class members’ data.

12 214. In exchange for these benefits to Plaid, Plaintiffs and Class members received
13 nothing. In fact, Plaintiffs and Class members were impoverished because, in order to benefit its
14 bottom line, Plaid sacrificed Plaintiffs’ and Class members’ financial security and privacy, and
15 violated their dignitary rights by perpetrating its deception.

16 215. Plaintiffs and Class members have suffered actual harm, including the increased
17 risk of the loss or theft of their financial data and the dignitary harms inherent in the intrusion of
18 personal privacy.

19 216. Plaintiffs and the Class seek an order that Plaid disgorge the profits and other
20 benefits it has unjustly obtained.

21 **SIXTH CAUSE OF ACTION**

22 **Violation of Cal. Bus. & Prof. Code § 17200 et seq.**

23 217. Plaintiffs incorporate the substantive allegations contained in all prior and
24 succeeding paragraphs as if fully set forth herein.

25 218. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class
26 (referred to in this claim as “the Class”).

27 219. California law applies to the Class here because California has significant contacts,
28 or significant aggregation of contacts, to the claims of each Class member, including that Plaid is

1 a California company with its headquarters in California, and conducts substantial business in
2 California. Additionally, the scheme described herein originated in California and the conduct
3 alleged herein emanated from California. And, upon information and belief, Class members' data
4 is pulled, stored, and aggregated by Plaid in California.

5 220. Plaid's conduct as alleged herein constitutes unfair, unlawful, or fraudulent
6 business acts or practices as prohibited by California's Unfair Competition Law, Cal. Bus. &
7 Prof. Code § 17200, *et seq.* (the "UCL").

8 **A. "Unlawful" Prong of the UCL**

9 221. Plaid's conduct is "unlawful" under the UCL. Plaid violated the Computer Fraud
10 and Abuse Act, 18 U.S.C. § 1030; the Stored Communications Act, 18 U.S.C. § 2701;
11 California's Comprehensive Data Access and Fraud Act, Cal. Pen. Code § 502; California's Anti-
12 Phishing Act of 2005, Cal. Bus. & Prof. Code § 22948.2; the GLBA's Privacy Rule, 16 C.F.R.
13 Part 313, and Reg. P, 12 C.F.R. Part 1016; Cal. Civ. Code § 1709; and Article 1, § 1 of the
14 California Constitution.

15 **B. "Unfair" Prong of the UCL**

16 222. Plaid's conduct also is "unfair" under the UCL. California has a strong public
17 policy of protecting consumers' privacy interests, including protecting consumers' banking data.
18 Plaid violated this public policy by, among other things, surreptitiously collecting Plaintiffs' and
19 Class members' private bank login information, using that login information to access their bank
20 accounts, accessing and copying Plaintiffs' and Class members' private banking data, selling and
21 transferring that data to Venmo and other fintech clients, and storing and using that data for its
22 own purposes, all without Plaintiffs' and Class members' consent.

23 223. Plaid's conduct also violated the important public interests protected by the
24 Computer Fraud and Abuse Act, 18 U.S.C. § 1030; the Stored Communications Act, 18 U.S.C.
25 § 2701; California's Comprehensive Data Access and Fraud Act, Cal. Pen. Code § 502;
26 California's Anti-Phishing Act of 2005, Cal. Bus. & Prof. Code § 22948.2; the GLBA's Privacy
27 Rule, 16 C.F.R. Part 313, and Reg. P, 12 C.F.R. Part 1016; Cal. Civ. Code § 1709; and Article 1,
28 § 1 of the California Constitution.

1 224. Plaintiffs and Class members did not anticipate and could not have anticipated this
2 degree of intrusion into their privacy. Plaid’s conduct did not create a benefit that outweighs these
3 strong public policy interests. Rather, Plaid’s conducts narrowly benefitted Plaid and its fintech
4 clients at the expense of the privacy of tens of millions of people. In addition, the effects of
5 Plaid’s conduct were comparable to or substantially the same as the conduct forbidden by the
6 California Constitution and the common law’s prohibitions against invasion of privacy, in that
7 Plaid’s conduct invaded fundamental privacy interests.

8 **C. “Fraudulent” Prong of the UCL**

9 225. Plaid’s conduct is “fraudulent” under the UCL. Plaid makes a practice of spoofing
10 bank websites in the software it incorporates into the Participating Apps for the purpose of
11 surreptitiously collecting consumers’ private bank login information, without the consumers’
12 knowledge or consent. Plaid also makes a practice of using consumers’ private bank login
13 information to access their bank accounts, accessing and copying Plaintiffs’ and Class members’
14 private banking data, selling and transferring that data to the Participating Apps, and storing and
15 using that data for its own purposes, all without the consumers’ knowledge or consent. These
16 business practices are likely to deceive members of the public and, indeed, have accomplished
17 widespread public deception.

18 **D. Plaintiffs’ Injuries and Rights to Relief**

19 226. Plaintiffs and Class members suffered injury in fact and lost money and /or
20 property as the result of Plaid’s unfair, unlawful, and fraudulent business practices, including
21 when:

22 a. Plaid removed Plaintiffs’ and Class members’ banking data from the secure
23 banking environment, selling or transferring it to the Participating Apps and storing it for Plaid’s
24 own use. Plaid thereby (1) destroyed the valuable indemnification rights Plaintiffs and Class
25 members had against loss when that data was in the banking environment; and (2) removed
26 valuable additional protections (including regulatory protections) Plaintiffs and Class members
27 had when that data was in the banking environment.
28

1 b. Plaid misappropriated Plaintiffs’ and Class members’ property in the form of their
2 exclusive records of their banking activities, sold it, and stored and used it for its own purposes.

3 227. As a result of Plaid’s violations of the UCL, Plaintiffs and Class members are
4 entitled to restitution, disgorgement by Plaid of the wrongfully-obtained private data obtained
5 from their financial accounts, including without limitation a return of that data to Plaintiffs and
6 Class members and the Plaintiffs’ and Class members’ financial institutions with corresponding
7 protections and security, and injunctive relief as prayed for below.

8 228. Section 17203 of the UCL authorizes a court to issue injunctive relief “as may be
9 necessary to prevent the use or employment by any person of any practice which constitutes
10 unfair competition.” Plaintiffs and Class members seek injunctive relief as prayed for below.

11 **SEVENTH CAUSE OF ACTION**

12 **Violation of Article I, Section I of the California Constitution**

13 229. Plaintiffs incorporate the substantive allegations contained in all prior and
14 succeeding paragraphs as if fully set forth herein.

15 230. Plaintiffs bring this claim on behalf of themselves and the California Class.

16 231. The California Constitution expressly provides for and protects the right to privacy
17 of California citizens: “All people are by nature free and independent and have inalienable rights.
18 Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting
19 property, and pursuing and obtaining safety, happiness, and privacy.” Cal. Const., art. I, § 1.

20 232. Plaintiffs and California Class members have a reasonable expectation of privacy
21 in their confidential financial affairs, including without limitation in the personal information and
22 banking data maintained at their financial institutions. Plaintiffs and California Class members
23 reasonably expected that their login credentials, account numbers, balances, transaction history,
24 and other information was private and secure within the institutions at which they maintain
25 accounts. They reasonably expected that their information and data (a) would be protected and
26 secured against access by unauthorized parties; (b) would not be obtained by unauthorized
27 parties; (c) would not be transmitted or stored outside of the secure bank environment; and
28 (d) would not be sold or used without their knowledge or permission.

1 233. Plaintiffs and California Class members have a legally protected privacy interest in
2 preventing the unauthorized access, dissemination, sale, and misuse of their sensitive and
3 confidential banking information and data.

4 234. Plaid intentionally violated Plaintiffs' and California Class members' privacy
5 interests. Plaid intruded upon Plaintiffs' and California Class members' sensitive and confidential
6 banking information in a manner sufficiently serious in nature, scope, and actual or potential
7 impact to constitute an egregious breach of the social norms underlying the privacy right.

8 235. Plaid intentionally violated Plaintiffs' and California Class members' privacy
9 interests by improperly accessing, downloading, transferring, selling, storing and using their
10 private banking information and data.

11 236. Plaid's violations of Plaintiffs' and California Class members' privacy interests
12 would be highly offensive to a reasonable person, especially considering (a) the highly sensitive
13 and personal nature of Plaintiffs' and California Class members' banking information and data;
14 (b) the extensive scope of data obtained by Plaid, including years of historical transactional data;
15 (c) Plaid's intent to profit from Plaintiffs' and California Class members' data by selling it
16 outright and using it to develop further products and services; and (d) the fact that Plaid used
17 subterfuge to intrude into Plaintiffs' and California Class members' banks' secure environment
18 for the purpose of collecting their data. Plaid's intrusions were substantial and constituted an
19 egregious breach of social norms.

20 237. Plaintiffs and California Class members did not consent to Plaid's violations of
21 their privacy interests.

22 238. Plaintiffs and California Class members suffered actual and concrete injury as a
23 result of Plaid's violations of their privacy interests. Plaintiffs and California Class members are
24 entitled to appropriate relief, including damages to compensate them for the harm to their privacy
25 interests, loss of valuable rights and protections, heightened risk of future invasions of privacy,
26 and the mental and emotional distress and harm to human dignity interests caused by Plaid's
27 invasions, as well as disgorgement of profits made by Plaid as a result of its violations of their
28 privacy interests.

1 from financial institutions rather than a third-party data aggregator, without obtaining the
2 authority or approval of each financial institution. Plaid successfully designed the interfaces to
3 mimic the login websites of financial institutions by using the banks' logos and color schemes, by
4 presenting each interface in the context of verifying ownership of a financial account, by
5 presenting each interface in a fashion that mirrored the experience of standard OAuth procedures
6 wherein consumers *are* communicating in a secure manner with their financial institutions, and
7 by failing to provide warnings and disclosures that a reasonable consumer would expect to
8 receive when their financial institution login credentials are requested by any party *other* than
9 their own financial institution. Each of these unlawful acts by Plaid was done without obtaining
10 the authority or approval of each financial institution in order to cause Plaintiffs and California
11 Class members to believe they were communicating with their financial institutions, and to thus
12 to obtain Plaintiffs' and California Class members' identifying information. Through these
13 means, Plaid did obtain Plaintiffs' and California Class members' bank login information.

14 245. Plaintiffs and California Class members have been adversely affected by Plaid's
15 violation of Section 22948.2 because they are the direct and intended victims of Plaid's phishing.
16 Each Plaintiff and California Class member provided their identifying information to Plaid under
17 false pretenses and was injured because Plaid obtained that information by deceiving them.
18 Plaintiffs and California Class members are also adversely affected by Plaid's conduct in using
19 their identifying information, including without limitation because Plaid accessed the sensitive
20 information stored in their financial accounts, and because Plaid used that information to acquire
21 profits and other benefits for itself, unjustly under the circumstances, and at the expense of the
22 security of Plaintiffs' and California Class members' financial information as compared to when
23 the information was solely accessible to each individual account holder and their financial
24 institution, as alleged herein.

25 246. Plaintiffs and California Class members are entitled to relief under Cal. Bus. &
26 Prof. Code § 22948.3(a)(2), including the following:

27 a. Injunctive relief as prayed for below;

28

1 credentials, including without limitation about the extent, duration, and consistency of Plaid’s
2 collection of private data from their financial accounts. Plaid’s omissions and nondisclosures
3 described herein were likely to deceive reasonable consumers, and have deceived Plaintiffs and
4 the California Class. Plaid’s acts of deceit include without limitation the following:

5 a. Plaid designed the software incorporated into the Participating Apps so that it
6 would deceive consumers as to the existence of Plaid as a separate entity, Plaid’s status as a third
7 party, and the nature of Plaid’s role as a data aggregator. Plaid suppresses these facts while under
8 a duty to disclose them.

9 b. In Plaid’s software incorporated in the Participating Apps, Plaid makes multiple
10 statements that are misleading and give rise to a duty to disclose the true state of affairs to
11 consumers. In the Venmo and Coinbase apps, for example (as in every Participating App
12 utilizing the template forms designed by Plaid), one such statement promises that the system is
13 “private,” and that the consumer’s “credentials will never be made accessible” to Venmo or
14 Coinbase. Plaid makes this statement while knowing that the system is designed not to be private
15 because it involves passing credentials to Plaid as a third-party data aggregator, and involves the
16 acquisition by third parties of the consumer’s most private banking data. By stating that the login
17 credentials will not be made accessible to Venmo or Coinbase, consumers are falsely led to
18 believe that their credentials are not shared outside of the bank they know and trust, while Plaid
19 in fact knows those credentials are intercepted by Plaid for its use in connecting to the bank.
20 Another misleading statement in the Plaid software incorporated in the Venmo and Coinbase
21 apps promises that the system is “Secure,” and that the consumer’s information is “encrypted
22 end-to-end.” In fact, Plaid knows that the system is designed not to be secure, including because
23 (1) Plaid uses it to collect, sell, use, and store consumers’ most private financial data; (2) Plaid
24 fails to exercise control or oversight over how that data is stored or used after it sells it to its
25 clients; and (3) when Plaid removes consumer banking data from the secure banking
26 environment, it thereby destroys valuable protections afforded to consumers in the event of data
27 breach/theft. And by stating that the consumer’s information is encrypted end-to-end, consumers
28 are falsely led to believe that no entity outside of each Participating App and the bank ever

1 receives access to any consumer information. At the same time Plaid makes the foregoing
2 statements, Plaid simultaneously suppresses the true facts while under a duty to disclose them.

3 c. In Plaid’s software incorporated in the Participating Apps, Plaid makes a practice
4 of spoofing bank login websites for the purpose of deceiving consumers into believing they are
5 logging into their bank, when in fact they are passing their bank login information directly to
6 Plaid. Plaid thereby suggests to consumers that they are entering their bank login information in
7 a secure manner, when Plaid knows that is not true.

8 d. In its privacy policy, Plaid intentionally conceals and fails to disclose (1) the fact
9 that Plaid collects consumer bank login information directly, (2) the fact that Plaid uses bank
10 login information to access consumers’ accounts, (3) the fact that Plaid collects all available
11 banking data from every available account once it accesses the original account; (4) the fact that
12 Plaid sells the consumer banking data it collects to the Participating Apps; (5) the fact that Plaid
13 does not exercise adequate oversight over how consumer banking data is stored or used after it
14 sells that data to the Participating Apps; (6) the fact that Plaid otherwise uses and monetizes the
15 consumer banking data it collects; (7) the fact that Plaid stores the consumer banking data it
16 collects; (8) the fact that the Participating Apps purchase, use, and store the consumer banking
17 data collected by Plaid; (9) the fact that Plaid continues to access accounts and collect, sell and
18 use consumer banking data long after the initial connection is made, regardless of whether the
19 consumer uses the Participating Apps; and (10) the fact that, by removing consumer banking
20 data from the secure banking environment, Plaid is destroying valuable indemnification rights
21 afforded to consumers. Plaid suppresses those facts while under a duty to disclose them.

22 e. Plaid falsely states in its privacy policy that the information it receives from banks
23 “varies depending on the specific Plaid services developers use to power their applications.” In
24 fact, Plaid knows that it collects all available consumer banking information when it connects
25 with a consumer’s bank, regardless of the services the Participating Apps choose to use.

26 f. By stating in the Plaid privacy policy that Plaid collects “[i]nformation about
27 account transactions, including amount, date, payee, type, quantity, price, location, involved
28 securities, and a description of the transaction,” Plaid intentionally deceives consumers who use

1 the Participating Apps into believing that Plaid only collects information about transactions
2 conducted using the Participating Apps. Plaid thereby suppresses the fact that it collects years'
3 worth of transactions entirely unrelated to the consumer's use of the Participating Apps, while
4 giving information of other facts which are likely to mislead for want of communication of that
5 fact.

6 252. Plaid's omissions and nondisclosures were pervasive. Plaintiffs and the California
7 Class members have reasonably relied on the material omissions and nondisclosures made by
8 Plaid.

9 253. Plaid's misconduct alleged herein was intentional, deliberate, and willful, and was
10 perpetrated with the intent to, *inter alia*, cause Plaintiffs and the California Class members
11 unknowingly to divulge confidential login credentials that could be and were used by Plaid to
12 access and collect private information stored within their financial accounts. Plaid thereby
13 willfully deceived Plaintiffs and California Class members with the intent to induce them to alter
14 their position to their injury or risk under Cal. Civ. Code § 1709.

15 254. Plaintiffs seek recovery of their and the California Class members' resulting
16 damages, including economic damages, restitution, and disgorgement, as well as punitive
17 damages.

18 **TENTH CAUSE OF ACTION**

19 **Violation of California's Comprehensive Data Access and Fraud Act, Pen. Code § 502**

20 255. Plaintiffs incorporate the substantive allegations contained in all prior and
21 succeeding paragraphs as if fully set forth herein.

22 256. Plaintiffs bring this claim on behalf of themselves and the California Class.

23 257. Plaid violated California Penal Code § 502(c)(1) by knowingly accessing and
24 without permission damaging and using both Plaintiffs' and California Class members' financial
25 institutions' computer systems and their data contained therein, in order to (i) execute Plaid's
26 scheme to defraud and deceive by wrongfully collecting, selling and using Plaintiffs' and
27 California Class members' private data, and (ii) wrongfully obtain money, as well as Plaintiffs'
28 and California Class members' valuable property and data.

1 258. Plaid violated California Penal Code § 502(c)(2) by knowingly accessing and
2 without permission taking, copying, and making use of Plaintiffs' and California Class members'
3 private data from Plaintiffs' and California Class members' financial institutions' computers,
4 computer systems, or computer networks.

5 259. Plaid violated California Penal Code § 502(c)(3) by knowingly and without
6 permission causing to be used Plaintiffs' and California Class members' financial institutions'
7 computer services.

8 260. Plaid violated California Penal Code § 502(c)(4) by knowingly accessing and
9 without permission damaging the integrity of Plaintiffs' and California Class members' financial
10 institutions' computer systems, as well as Plaintiffs' and California Class members' data
11 contained therein.

12 261. Plaid violated California Penal Code § 502(c)(6) by knowingly and without
13 permission providing a means for the Participating Apps to access Plaintiffs' and California Class
14 members' financial institutions' computer systems in violation of Penal Code Section 502 by
15 using its software to surreptitiously collect Plaintiffs' and California Class members' bank login
16 information, using it to establish connections to Plaintiffs' and California Class members' banks,
17 and then selling access tokens to the Participating Apps so they could access and download
18 Plaintiffs' and California Class members' private banking data.

19 262. Plaid violated California Penal Code § 502(c)(7) by knowingly and without
20 permission accessing Plaintiffs' and California Class members' banks' computer systems.

21 263. Plaintiff violated California Penal Code § 502(c)(8) by knowingly introducing a
22 computer contaminant into Plaintiffs' and California Class members' smartphones, in the form of
23 the software it incorporated into the apps of the Participating Apps, to surreptitiously collect
24 Plaintiffs' and California Class members' financial institution login information.

25 264. None of Plaintiffs, California Class members, nor Plaintiffs' and California Class
26 members' financial institutions gave express or implied permission to Plaid to access their
27 financial institutions' computer systems or the data stored therein. Plaintiffs and California Class
28 members did not give express or implied permission to Plaid to access their smartphones.

1 265. Plaid accessed Plaintiffs’ and California Class members’ private banking data,
2 Plaintiffs’ and California Class members’ banks’ computer systems, and Plaintiffs’ and California
3 Class members’ smartphones in a manner that circumvented technical or code-based barriers in
4 place to restrict or bar third-party access.

5 266. As the owners of the private data that is the subject of this cause of action and
6 persons who suffered damage or loss by reason of Plaid’s above violations, Plaintiffs and
7 California Class members are entitled under California Penal Code § 502(e) to pursue an action
8 against Plaid for compensatory damages and injunctive relief or other equitable relief, as well as
9 to recover reasonable attorneys’ fees. And because Plaid’s violations were willful and Plaid is
10 guilty of oppression, fraud, or malice, Plaintiffs and California Class members also are entitled to
11 an award of punitive or exemplary damages.

12 **PRAYER FOR RELIEF**

13 WHEREFORE, Plaintiffs request that judgment be entered against Plaid and that the
14 Court grant the following:

15 A. An order determining that this action may be maintained as a class action under
16 Rule 23 of the Federal Rules of Civil Procedure, that Plaintiffs are Class Representatives, that
17 Plaintiffs’ attorneys shall be appointed as Class Counsel pursuant to Rule 23(g) of the Federal
18 Rules of Civil Procedure, and that Class notice be promptly issued;

19 B. Judgment against Plaid for Plaintiffs’ and Class members’ asserted claims for
20 relief;

21 C. Appropriate declaratory relief against Plaid;

22 D. Equitable and injunctive relief requiring Plaid to: (1) purge the data it has
23 unlawfully collected; (2) plainly and conspicuously disclose, on the first screen of its Plaid Link
24 software, if and when presented to consumers, (a) that Plaid is a third party data aggregator
25 providing connection services to consumers’ financial institutions for the purpose of collecting
26 private data from their financial institutions, (b) that it is not necessary for consumers to connect
27 to their banks using Plaid; and (c) that using Plaid’s services will eliminate consumers’
28 indemnification rights provided by financial institutions; (3) obtain, before it connects with a

1 consumer's financial account, affirmative permission from the consumer for each action Plaid
2 takes in connection with the account, including accessing, copying, selling, storing, and using
3 data; (4) before it connects with a consumer's financial account, require the consumer to review
4 the full text of Plaid's privacy policy, acknowledge all of the terms and conditions by checking
5 boxes to indicate their consent to those provisions, and acknowledge receipt and approval of the
6 notice; (5) obtain a consumer's affirmative consent each time Plaid accesses that consumer's
7 financial account and financial data; and (6) notify consumers of Plaid's actions to remedy its
8 unlawful conduct alleged herein, and steps consumers can take to prevent future and additional
9 privacy invasions by Plaid and other actors to whom Plaid has sold or otherwise delivered their
10 personal information;

11 E. Equitable and injunctive relief enjoining Plaid from: (1) accessing, attempting to
12 access, or procuring transmission of any California Class member's identifying information
13 through their financial accounts; (2) representing that any solicitation, request, or action by Plaid
14 is being done by a financial institution; (3) retaining any copies, electronic or otherwise, of any
15 identifying information obtained through the phishing scheme alleged herein; (4) retaining any
16 copies, electronic or otherwise, of any other information obtained from any of Plaintiffs' or
17 California Class members' financial institutions using identifying information obtained through
18 the phishing scheme alleged herein; and (5) engaging in any unlawful activities alleged herein;

19 F. An order awarding Plaintiffs and the Class members actual and/or statutory and/or
20 special and/or incidental damages as well as restitution;

21 G. An order requiring Plaid to pay punitive damages, dignitary damages, and
22 exemplary damages;

23 H. An order requiring Plaid to pay pre-judgment and post-judgment interest;

24 I. Reasonable attorney's fees and costs reasonably incurred; and

25 J. Any and all other and further relief to which Plaintiffs and the Classes may be
26 entitled.

27 //

28 //

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury of all issues so triable.

Dated: May 4, 2020

HERRERA PURDY LLP

By: /s/ Shawn Kennedy
Shawn M. Kennedy

Shawn M. Kennedy (SBN 218472)
skennedy@herrerapurdy.com
Andrew M. Purdy (SBN 261912)
apurdy@herrerapurdy.com
Bret D. Hembd (SBN 272826)
bhembd@herrerapurdy.com
4590 MacArthur Blvd., Suite 500
Newport Beach, CA 92660
Tel: (949) 936-0900
Fax: (855) 969-2050

HERRERA PURDY LLP
Nicomedes Sy Herrera (SBN 275332)
nherrera@herrerapurdy.com
Laura E. Seidl (SBN 269891)
lseidl@herrerapurdy.com
1300 Clay Street, Suite 600
Oakland, California 94612
Telephone: (510) 422-4700

LIEFF CABRASER HEIMANN &
BERNSTEIN, LLP

By: /s/ Michael Sobol
Michael W. Sobol

Michael W. Sobol (SBN 194857)
msobol@lchb.com
Melissa Gardner (SBN 289096)
mgardner@lchb.com
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Tel: (415) 956-1000
Fax: (415) 956-1008

LIEFF CABRASER HEIMANN &
BERNSTEIN, LLP
Rachel Geman (*Pro Hac Vice* to be Filed)
rgeman@lchb.com
250 Hudson Street, 8th Floor
New York, NY 10013-1413
Tel: (212) 355-9500
Fax: (212) 355-9592

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

LIEFF CABRASER HEIMANN &
BERNSTEIN, LLP
Madeline M. Gomez (*Pro Hac Vice* to be Filed)
mgomez@lchb.com
222 2nd Avenue South, Suite 1640
Nashville, TN 37201
Tel: (615) 313-9000
Fax: (212) 313-9965

BURNS CHAREST LLP

By: /s/ Christopher Cormier
Christopher J. Cormier

Christopher J. Cormier (*Pro Hac Vice* to be Filed)
ccormier@burnscharest.com
5290 Denver Tech Center Parkway, Suite 150
Greenwood Village, CO 80111
Tel: (720) 630-2092
Fax: (469) 444-5002

BURNS CHAREST LLP
Warren T. Burns (*Pro Hac Vice* to be Filed)
wburns@burnscharest.com
Russell Herman (*Pro Hac Vice* to be Filed)
rherman@burnscharest.com
900 Jackson Street, Suite 500
Dallas, TX 75202
Tel: (469) 904-4550
Fax: (469) 444-5002

BURNS CHAREST LLP
C. Jacob Gower (*Pro Hac Vice* to be Filed)
jgower@burnscharest.com
365 Canal Street, Suite 1170
New Orleans LA 70130
Tel: (504) 799-2845
Fax: (504) 881-1765

Attorneys for Plaintiffs and the Proposed Classes