EXHIBIT A

HERRERA PURDY LLP
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, CA 94612
Tel: (510) 422-4700
Fax: (855) 969-2050

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

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

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
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

Attorneys for Plaintiffs and the Proposed Classes

[Additional counsel on signature page]

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

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

Plaintiffs,

v.

PLAID INC., a Delaware corporation,

Defendant.

Case No.: _____

COMPLAINT FOR DAMAGES AND DECLARATORY AND EQUITABLE RELIEF

CLASS ACTION

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

Page

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

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

I. INTRODUCTION

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

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

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

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

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

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

II. JURISDICTION AND VENUE

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

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

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

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

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

III. INTRADISTRICT ASSIGNMENT

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

IV. THE PARTIES

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

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

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

[1] *See* https://plaid.com/company/.

V. FACTUAL BACKGROUND

A. Background of Plaid and the Participating Apps

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

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

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

---

[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.

[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.

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

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

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

---

[4] *See* https://news.ycombinator.com/item?id=5216710.

[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.

[6] *See* https://news.ycombinator.com/item?id=5304169.

[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.

[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 ("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.").

[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 corporate entity registered in New York (Venmo LLC). In 2015, Venmo was acquired by PayPal, Inc. and subsequently merged with that corporation.

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

B. Plaid Deceptively Obtains Bank Account Credentials from App Users

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

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

---

[10] *See* https://investor.paypal-corp.com/static-files/0b7b0dda-a4ee-4763-9eee-76c01be0622c.

[11] *See* https://www.coinbase.com/about.

[12] *See* https://www.businessinsider.com/squares-cash-app-reached-24-million-users-and-monetization-surge-2020-2.

[13] *See* https://www.stripe.com/customers.

[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.

app.[15] Behind the scenes, the bank returns a "token" that allows the original app to access the consumer's bank information as necessary and authorized by the consumer, but without giving the app provider access to the login information.

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

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

26. Plaid refers to this new method as a "Managed OAuth" system. Plaid's Managed OAuth process has been incorporated in its "Plaid Link" software, which consists of software, including login screens, developed by Plaid and distributed to its fintech clients for incorporation into their apps.[19]

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

---

[15] *See, e.g.*, https://www.oauth.com/oauth2-servers/redirect-uris/.

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

[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/.

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





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

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

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

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

---

[20] *See* Jun. 20, 2016 Y Combinator Hacker News thread: *Fintech Firm Plaid Raises $44M*, https://news.ycombinator.com/item?id=11939103.

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

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

> [Programmer]: givelively.org prompts me to provide my banking password on a web donation page. Browser inspector shows it's putting up a plaid.com iframe. That even renders my bank's logo to fool me into thinking I'm accessing my bank's site. This is absolutely unacceptable, regardless of what claims you make on your security page.
>
> [Michael Kelly]: [W]e appreciate your concerns, which is why our compliance team vets anybody who uses Link. As to malicious knock offs, this is a matter that most successful companies lookout for and deal with -- as we and our security team do. If you see someone impersonating Link in such a way, please drop us a note at security@plaid.com. It's also worth noting that, in addition to the security we provide, banks protect their users from credential-based attacks via multi factor authentication. [23]

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

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

> [User]: "I would really caution connecting your bank account through Plaid on [Robinhood]. It's really unclear what data they are collecting but their privacy policy suggests they are collecting your bank account transaction history using Plaid's API. 100% a dealbreaker for me."
>
> [Hockey]: "[C]o-founder of Plaid here. I can't give the rationale on why RH wrote the privacy policy the way they did, but I can guarantee you that they are not pulling transactional data. They're only using Plaid for the ACH authentication."[24]

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

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

---

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

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

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

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

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

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

[25] *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, at 12.

[26] *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/.

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

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

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

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

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

---

[27] *See* May 13, 2019 interview with Zach Perret at Data Driven NYC event at 16:34 to 17:19, https://www.youtube.com/watch?v=sgnCs34mopw; *see also* 12 U.S.C. § 5533 (Dodd-Frank Act 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

41. As a result, even as early as February 2013, Plaid's co-founders could tell industry insiders that the company was "generating one of the largest transactional data sets in the world."[29]

42. Plaid generated this data set by engaging in still more unfair and unethical behavior. Plaid circumvented counter-measures employed by some banks to prevent data aggregators like Plaid from siphoning all information in a given consumer's accounts by accessing accounts with the consumer's credentials and "scraping" (*i.e.*, copying) data the banks would not share directly. Plaid's insiders understood the unethical nature of the company's method of gaining access to banks' data stores. In August 2018, a former Plaid programmer responded to a Hacker News thread titled, *What is the most unethical thing you've done as a programmer?* The programmer identified his work for Plaid as one of the most unethical things he had ever done because, after consumers' login credentials were obtained, Plaid developed methods for bypassing banks' protections against data scraping[30] by using their status as an "affiliate" of banks' downstream clients:

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

---

at 5:51 to 7:50, https://www.youtube.com/watch?v=_I8DRbFmLKM.

[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.

> of analytics on customer data acquired as part of the account verification process.
>
> . . .
>
> I don't have an issue with user data being mined for things like market research if it's a situation where the product is free and users can be easily made aware of it. But I find it dishonest if the company mining that data is doing so without direct user consent, or in a "backdoored" manner using their status as a downstream client's "affiliate" for T&C purposes.[31]

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

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

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

---

[31] *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.

[32] *See* May 13, 2019 interview with Zach Perret at Data Driven NYC event at 11:53 to 12:05, 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/.

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

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

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

47. In the January 13, 2020 press release and accompanying presentation announcing Visa's purchase of Plaid, Visa reiterated that Plaid has the banking information of one in four people with a U.S. bank account, including the banking data from over 200 million accounts.[36] Venmo users alone accounted for a large portion of those consumers and accounts, given that Venmo had over 52 million users as of the end of 2019.[37]

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

---

[35] *See* https://plaid.com/docs/legacy/api/.

[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.

[37] *See* https://investor.paypal-corp.com/static-files/0b7b0dda-a4ee-4763-9eee-76c01be0622c.

[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-

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

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

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

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

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

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

---

Presentation.pdf.

[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 sells data to party "permissioned" by consumer).

[41] *See* Feb. 2019 interview with Zach Perret, https://www.saastr.com/build-a-platform-ecosystem/.

[42] *See* https://plaid.com/legal/.

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

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

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

---

[43] *See* Jul. 1, 2015 Y Combinator Hacker News thread, https://news.ycombinator.com/item?id=9812245.

[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.

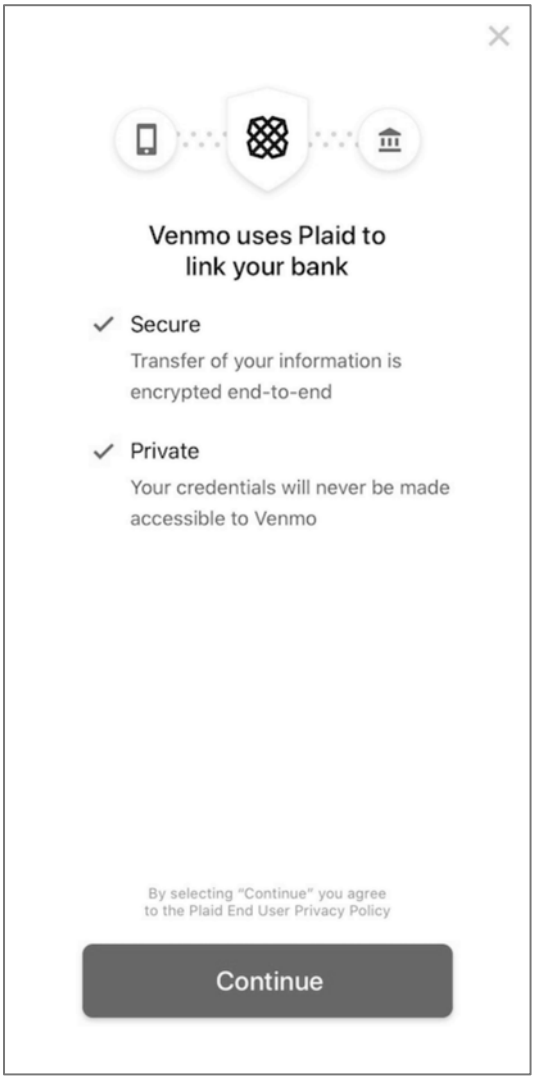
[45] *See* May 13, 2019 interview with Zach Perret at Data Driven NYC event at 14:21 to 14:26, https://www.youtube.com/watch?v=sgnCs34mopw.

[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-that-powers-venmo-robinhood-and-other-big-apps.html.

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.

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



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

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

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

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

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

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

[47] Plaid's privacy policy is no better disclosed to users of other Participating Apps. The screens 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."

> applications, as well as the information made available by those providers. But, in general, we collect the following types of identifiers, commercial information, and other personal information from your financial product and service providers:
>
> - Account information, including financial institution name, account name, account type, account ownership, branch number, IBAN, BIC, and account and routing number;
> - Information about an account balance, including current and available balance;
> - Information about credit accounts, including due dates, balances owed, payment amounts and dates, transaction history, credit limit, repayment status, and interest rate;
> - Information about loan accounts, including due dates, repayment status, balances, payment amounts and dates, interest rate, guarantor, loan type, payment plan, and terms;
> - Information about investment accounts, including transaction information, type of asset, identifying details about the asset, quantity, price, fees, and cost basis;
> - Identifiers and information about the account owner(s), including name, email address, phone number, date of birth, and address information;
> - Information about account transactions, including amount, date, payee, type, quantity, price, location, involved securities, and a description of the transaction; and
> - Professional information, including information about your employer, in limited cases where you've connected your payroll accounts.
>
> 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

---

[49] *See* https://plaid.com/pricing/.

[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#.XksqMxNKjQg.

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

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

F. Plaid's Harm to Consumers is Recognized by Banks and Industry Groups

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

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

[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).

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

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

> (a) Unknowing Grant of Unlimited Access
>
> "Current practices in the data aggregation market . . . may leave consumers exposed and create risk that undermine this trust. Consumers today are offered a Faustian bargain in which their desire for technology-driven convenience is exchanged—often unknowingly—for increased potential of catastrophe, by handing over the keys to their financial vault. When consumers share their login credentials with an aggregator, they are giving the aggregator *carte blanche* access to their financial data, including information about things such as their life savings or retirement account. Yet consumers are not given adequate information or control over what information is being taken, how long it is accessible, and how it will be used in the future."[54]
>
> (b) Unknowing Removal of Sensitive Information from Secure Environment
>
> "Moreover, consumers are unaware of the differences in the legal and supervisory standards applicable to bank and nonbank participants in the financial services marketplace. Once the information is shared, it leaves a secure bank environment, where it is accorded longstanding legal protections, and it is released into the data services market where it is accorded no more special status than data created through a consumer's use of a social media platform.
>
> . . .
>
> When consumers allow data aggregators to access their data they run the risk – often unknowingly – associated with moving their data out of the secure banking environment, where it is fully protected by law, and moving it into the data services market where it is not accorded 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.

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

(c) Access Unlimited as to Scope or Time

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

(d) Access to Unnecessary Data

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

(e) Use and Sale of Banking Data

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

(f) Increased Risk of Identity Theft

"The risks to consumers should not be minimized. First, the sheer volume and value of the aggregated data make data aggregators a priority target for criminals, including identity thieves. This is because data aggregators collect and share information from multiple financial institutions which is a vast expansion of the information held at any one bank. Thus, data aggregators may have the financial information, including account credentials, for the accounts across a consumer's entire financial portfolio. Through a single source, the criminal may gain access to the consumer's checking and savings accounts, retirement accounts, certificates of deposits, credit cards, 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

[55] *Id.*

[56] *Id.*

[57] *Id.*

[58] *Id.*

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

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

69. Larrimer further explained in a subsequent article that PNC's position is that many consumers do not fully understand what happens to their data when they sign up for an app, and an aggregator such as Plaid is involved behind the scenes. One thing many consumers do not recognize, Larrimer explained, is that once access has been obtained to one banking account, the aggregator "can scrape every piece of information that is in your banking relationships—any other accounts you have, any loans you have, any transaction data, whatever is there they have 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.

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

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

G. Plaid Knowingly Violates Established Industry Standards and Obligations

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

1. The GLBA Standards

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

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

[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/.

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

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

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

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

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

2. Plaid's Acknowledgement of Its Disclosure Obligations

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

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

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

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

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

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

---

[63] *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 (emphasis added).

[64] *See* https://web.archive.org/web/20160920005638/https://plaid.com/legal/ (emphasis added).

[65] *See* https://plaid.com/legal/.

> and newer digital players – should abide by this framework, including provisions that limit the use of permissioned data to the 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.
>
> . . .
>
> Beyond the letter of the law, both intermediaries and permissioned parties should also honor the principles of data minimization and consumer transparency. Consumers should know what data is being 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]

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

> Plaid represents a new approach enabled by modern technology, helping a consumer access their own data only when they chose to do so, and sharing it only with the companies they select. This is a consumer-permissioned model, in which consumers control what they do with their data.
>
> Consumer permission is the backbone of account connectivity. However, industry disclosure practices can and should be improved. At Plaid, consumer permission and control are core principles. Unlike many other service providers who rely on personal or financial data, our account connectivity services require consumers to affirmatively provide or permission access to their account information to the company they want to share it with.
>
> Most importantly, consumers should understand: What data is being shared? For what purpose? And what ability do they have to direct what happens to their data? At Plaid, we have developed simple, plain-English disclosures and privacy policies designed to help consumers understand which information is collected and how it is used, shared and stored. We have previously discussed the potential benefits of Schumer-box[67]-like disclosures for consumer data access, and believe Plaid—and the rest of the industry—should continue to develop and test more effective consumer disclosures.
>
> [C]onsumer permission should be tied to the services the consumer requests or purposes for which they are specifically informed when

---

[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).

[67] A Schumer Box, named after Senator Chuck Schumer, is an easy-to-read table or "box" that 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 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.

> they grant access. Affirmative permission (not fine-print click-through) should be required in order to sell account data, even in aggregated form, to any parties the consumer doesn't have a direct permissioning relationship with. To do otherwise would breach the 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]

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

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

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

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

---

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

[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.

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

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

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

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

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

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

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

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

VI. INJURY AND DAMAGES TO THE CLASS

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

A. The Named Plaintiffs' Experiences

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

B. Injuries from Invasions of Privacy and Dignitary Violations

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

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

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

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

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

[70] *See* https://plaid.com/docs/; https://web.archive.org/web/20160319102824/https://plaid.com/docs/.

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

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

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

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

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

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

---

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

[72] *Id.*

[73] *Id.* at 7.

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

C. Economic Damages

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

1. Loss of Valuable Indemnification Rights

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

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

111. Regulation E defines an "[u]nauthorized electronic fund transfer" as "an electronic fund transfer from a consumer's account initiated by a person other than the consumer without

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

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

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

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

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

---

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

[76] *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.

[77] *See* Apr. 6, 2016 Letter from JPMorgan Chase to shareholders, https://www.jpmorganchase.com/corporate/annual-report/2015/.

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

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

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

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

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

---

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.

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

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

2. Diminished Value of Rights to Protection of Data

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

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

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

3. Loss of Control Over Valuable Property

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

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

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

[80] *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.

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

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

4. Increased Risk of Identity Theft and Fraud

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

> [T]he sheer volume and value of the aggregated data make data aggregators a priority target for criminals, including identity thieves. . . . Through a single source, the criminal may gain access to the consumer's checking and savings accounts, retirement accounts, certificates of deposits, credit cards, brokerage accounts, 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]

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

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

[81] *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.

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

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

VII. CHOICE OF LAW

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

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

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

VIII. TOLLING, CONCEALMENT, AND ESTOPPEL

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

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

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

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

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

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

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

IX. CLASS ACTION ALLEGATIONS

139. Plaintiffs incorporate by reference all the foregoing allegations.

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

141. Plaintiffs seek to represent the following Classes:

> **Nationwide Class:** All natural persons in the United States whose accounts at a financial institution were accessed by Plaid using login credentials obtained through Plaid's software incorporated in a 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.
>
> **California Class:** All natural persons in California whose accounts at a financial institution were accessed by Plaid using login credentials obtained through Plaid's software incorporated in a 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.

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

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

144. Numerosity and Ascertainability: Plaintiffs do not know the exact size of the Classes or the identities of the Class members. Such information is known to Plaid. At minimum, each Class has thousands or millions of members. Reports indicate that Plaid has accessed approximately 200 million United States financial accounts. Venmo had over 52 million active accounts at the end of 2019.[82] Coinbase reportedly has more than 30 million users.[83] Square's Cash App reportedly has more than 24 million monthly active users.[84] Thus, the number of members in each Class is so numerous that joinder of all Class members is impracticable. The names, addresses, and phone numbers of Class members are identifiable through documents maintained by Plaid, and also available from the records of third parties such as Class members' financial institutions and the Participating Apps.

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

(1) Whether Plaid omitted or concealed material facts from Plaintiffs and Class members;

(2) Whether Plaid owes a duty to Plaintiffs and Class members to disclose material facts;

(3) Whether Plaid gave effective notice of its privacy policy under an

[82] *See* https://investor.paypal-corp.com/static-files/0b7b0dda-a4ee-4763-9eee-76c01be0622c.

[83] *See* https://www.coinbase.com/about.

[84] *See* https://www.businessinsider.com/squares-cash-app-reached-24-million-users-and-monetization-surge-2020-2.

objectively reasonable consumer standard;

(4) Whether Plaid's privacy policy discloses Plaid's conduct;

(5) Whether credentials obtained through Plaid's Managed OAuth procedure were obtained with Plaintiffs' and Class members' informed consent;

(6) Whether Plaid's use of Plaintiffs' and Class members' banking credentials obtained through Plaid's Managed OAuth procedure to access Plaintiffs' and Class members' financial institution accounts was done with Plaintiffs' and Class members' informed consent;

(7) Whether Plaid obtained broad financial data from Class members' bank accounts;

(8) Whether Plaid's acts and practices complained of herein amount to egregious breaches of social norms;

(9) Whether Plaid's conduct described herein violates Plaintiffs' and Class members' interest in precluding the dissemination or misuse of sensitive and confidential information ("informational privacy");

(10) Whether Plaid's conduct described herein violates Plaintiffs' and Class members' interest in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference ("autonomy privacy");

(11) Whether the computer systems operated by Plaintiffs' and Class members' financial institutions are "protected computers" or "computers of financial institutions" under the CFAA;

(12) Whether Plaid intentionally accessed protected computer systems in violation of the CFAA;

(13) Whether Plaid improperly obtained and disclosed Plaintiffs' and Class members' financial information without authorization or in

excess of any authorization;

(14) Whether Plaid knowingly trafficked in access tokens or similar information so the Participating Apps could access Plaintiffs' and Class members' private data from their financial institutions;

(15) Whether Plaid's conduct violated the Stored Communications Act, 18 U.S.C. § 2701, *et seq.*;

(16) Whether profits obtained by Plaid through sale of information or sale of access to information obtained from Plaintiffs' and Class members' financial accounts were unjustly obtained by Plaid and should be disgorged;

(17) Whether any profits or other value obtained by Plaid through analysis, enrichment, and other use of information from Plaintiffs' and Class members' financial accounts were unjustly obtained by Plaid and should be disgorged;

(18) Whether declaratory relief and an injunction should be granted;

(19) Whether Plaid's conduct violated the California Constitution;

(20) Whether Plaid, through its Managed OAuth process, induced California Class members to provide "identifying information" within the meaning of the California Anti-Phishing Act by representing itself to be a business without the authority or approval of the business;

(21) Whether Plaintiffs and Class members are "adversely affected" within the meaning of the California Anti-Phishing Act by the collection of their financial institution login credentials and identifying information by Plaid or by Plaid's subsequent use and sale of such information;

(22) Whether Plaid's conduct was an unlawful, unfair, or fraudulent business practice under Cal. Bus. & Prof. Code § 17200, *et seq.*;

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

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

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

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

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

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

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

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

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

X. CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION

Invasion of Privacy—Intrusion into Private Affairs

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SECOND CAUSE OF ACTION

Violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

G. Plaintiffs' Right to Recover Damages

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

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

THIRD CAUSE OF ACTION

Violation of the Stored Communications Act ("SCA"), 18 U.S.C. § 2701

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

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

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

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

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

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

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

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

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

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

200. Plaid's access to these facilities was achieved through subterfuge. Insofar as Plaid obtained purported authorization for its conduct, Plaid exceeded any such authorization by collecting, aggregating, selling, and divulging the contents of Plaintiffs' and Class members' electronic banking communications that were unrelated to the purpose for which Plaintiffs used the Participating Apps. 18 U.S.C. § 2701(a)(2). Plaid acquired communications far in excess of any information necessary to the Participating Apps for which account verification and linking were undertaken.

201. Plaintiffs and Class members are aggrieved by, and suffered concrete and particularized injury resulting from, Plaid's acquisition of their communications from financial institutions because they suffered economic, privacy, and human dignity harms as a result, as alleged herein, including without limitation at ¶¶ 102-29.

202. As persons aggrieved by Plaid's knowing and intentional violations of the SCA, Plaintiffs and Class members are entitled to appropriate relief under 18 U.S.C. § 2707, including (i) preliminary and other equitable or declaratory relief as prayed for below, (ii) damages, and (iii) reasonable attorneys' fees and costs.

a. For damages, Plaintiffs and Class members are entitled to recover their actual damages, as well as all profits made by Plaid as a result of their violations. In addition, because Plaid's violations of the SCA were willful or intentional, Plaintiffs and Class members also are entitled to punitive damages.

203. Plaintiffs and Class members bring this cause of action within two years after the date upon which they first discovered or had a reasonable opportunity to discover Plaid's violations under 18 U.S.C. § 2707(f).

FOURTH CAUSE OF ACTION

Declaratory Judgment that Plaid Wrongfully Accessed, Collected, Stored, Disclosed, Sold, and Otherwise Improperly Used Plaintiffs' Private Data and Injunctive Relief

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

205. Plaintiffs bring this claim on behalf of the Nationwide Class (referred to in this claim as "the Class").

206. The gravamen of this controversy lies in Plaid's failure to inform consumers of its true nature and conduct, and Plaid's subsequent invasions of their privacy. Plaintiffs and Class members never consented to sharing their bank login credentials with Plaid, never agreed to share their private, personal banking history and data with Plaid, never assented to Plaid gathering, storing, disclosing, selling, or otherwise using their private, personal data.

207. Plaid's misconduct has put Plaintiffs' and Class members' financial privacy and security at risk, and violated their dignitary rights, privacy, and economic well-being. Accordingly, Plaintiffs seek appropriate declaratory relief, and injunctive relief as prayed for below.

FIFTH CAUSE OF ACTION

Unjust Enrichment (Quasi-Contract Claim for Restitution and Disgorgement)

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

209. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class (referred to in this claim as "the Class").

210. Plaid has unjustly received benefits at the expense of Plaintiffs and the Class.

211. Plaid acquired and compromised the security of troves of private, personal banking records and transaction data that rightfully belong to Plaintiffs and the Class without informing them of these risks and through intentionally deceptive practices conducted in connection with consumers' use of the Participating Apps.

212. The unethical, unfair, and deceptive practices Plaid employed to acquire and compromise this information include, without limitation: mimicking bank interfaces to cause Plaintiffs and Class members reasonably to believe they were providing their login credentials to their financial institutions, rather than a third party company; disguising Plaid's appearance in the Participating Apps such that Plaintiffs and Class members were not made aware of the presence and conduct of a third party application; failing to correct material misleading information

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

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

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

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

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

SIXTH CAUSE OF ACTION

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

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

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

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

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

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

A. "Unlawful" Prong of the UCL

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

B. "Unfair" Prong of the UCL

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

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

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

C. "Fraudulent" Prong of the UCL

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

D. Plaintiffs' Injuries and Rights to Relief

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

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

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

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

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

SEVENTH CAUSE OF ACTION

Violation of Article I, Section I of the California Constitution

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

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

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

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

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

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

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

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

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

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

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

EIGHTH CAUSE OF ACTION

Violation of Anti-Phishing Act of 2005, Cal. Bus. & Prof. Code § 22948 *et seq.*

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

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

242. The California Anti-Phishing Act of 2005 ("CAPA"), Cal. Bus. & Prof. Code § 22948.2 prohibits deceptive procurement of personal information that can be used to access the financial accounts of California residents. CAPA provides that it is "unlawful for any person, by means of a Web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business." CAPA, Cal. Bus. & Prof. Code § 22948.1, defines "identifying information" to include, *inter alia*, bank account numbers, account passwords, and any other piece of information that can be used to access an individual's financial accounts.

243. Plaid acquired identifying information in the form of Plaintiffs' and California Class members' bank account usernames and password information, codes received through the financial institutions' two-factor authentication processes, and all other identifying information sufficient for Plaid to access Plaintiffs' and California Class members' financial accounts.

244. Plaid obtained this identifying information in violation of Cal. Bus. & Prof. Code § 22948.2 by engaging in a pattern and practice of deception over several years (from no later than 2016 to present) affecting tens or hundreds of millions of consumers, including Plaintiffs and California Class members, namely, by designing and presenting consumer-facing interfaces in which to enter financial account usernames and passwords to appear as though they originated

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

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

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

a. Injunctive relief as prayed for below;

b. An order requiring Plaid to account for, hold in constructive trust, pay over to Plaintiffs and the California Class, and otherwise disgorge all profits derived by Plaid from its unlawful conduct and unjust enrichment, as permitted by law;

c. An award to Plaintiffs and the California Class of damages, including but not limited to, compensatory, statutory, treble, exemplary, aggravated, and punitive damages, as permitted by law and in such amounts to be proven at trial;

d. An award to Plaintiffs of reasonable costs, including reasonable attorneys' fees;

e. For pre-and post-judgment interest as allowed by law; and

f. For such other relief as the Court may deem just and proper.

NINTH CAUSE OF ACTION

Violation of Cal. Civ. Code §§ 1709 & 1710

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

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

249. California Civil Code § 1709 provides that "[o]ne who willfully deceives another with intend to induce him to alter his position to his injury or risk, is liable for any damage which he thereby suffers."

250. California Civil Code § 1710 defines "deceit" as (1) the suggestion, as a fact, of that which is not true, by one who does not believe it to be true; (2) the assertion, as a fact, of that which is not true, by one who has no reasonable ground for believing it to be true; (3) the suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact; or (4) a promise, made without any intention of performing it.

251. Throughout the class period, Plaid engaged in deceit by intentionally concealing and failing to disclose its true nature and conduct to consumers. Plaid knew that representations made within the Participating Apps were misleading and material, and that the facts Plaid failed to disclose and concealed were material. Plaid owed a duty to Plaintiffs and the California Class to provide them material information about its acquisition and use of their financial account

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

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

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

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

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

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

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

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

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

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

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

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

TENTH CAUSE OF ACTION

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

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

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

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

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

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

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

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

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

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

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

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

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

PRAYER FOR RELIEF

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

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

B. Judgment against Plaid for Plaintiffs' and Class members' asserted claims for relief;

C. Appropriate declaratory relief against Plaid;

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

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

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

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

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

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

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

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

//

//

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

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