Michael F. Ram (SBN 104805)
Aaron M. Sheanin (SBN 214472)
mram@robinskaplan.com
asheanin@robinskaplan.com
ROBINS KAPLAN LLP
2440 W El Camino Real, Suite 100
Mountain View, CA 94040
Telephone: (650) 784-4040

Kellie Lerner (*Pro Hac Vice* to be filed)
Hollis Salzman (*Pro Hac Vice* to be filed)
William Reiss (*Pro Hac Vice* to be filed)
David Rochelson (*Pro Hac Vice* to be filed)
klerner@robinskaplan.com
hsalzman@robinskaplan.com
wreiss@robinskaplan.com
drochelson@robinskaplan.com
ROBINS KAPLAN LLP
399 Park Avenue, Suite 3600
New York, NY 10022
Telephone: (212) 980-7400

Attorneys for Plaintiff and the Proposed Classes

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

LOGAN MITCHELL, individually and on behalf of all others similarly situated, Plaintiff, v. PLAID INC., a Delaware corporation, Defendant.	Case No. ____ **COMPLAINT FOR DAMAGES AND DECLARATORY AND EQUITABLE RELIEF** **CLASS ACTION** **DEMAND FOR JURY TRIAL**

Plaintiff Logan Mitchell ("Plaintiff"), individually and as representative of a class of similarly situated persons, by her undersigned counsel, alleges as follows against Defendant Plaid Inc. ("Plaid"):

I. INTRODUCTION

1. Imagine there is a company that knows every dollar you deposit or withdraw, every

dollar you charge or pay to your credit card, and every dollar you put away for retirement, within hours after you make the transaction. Imagine this includes every book or movie ticket or meal you purchase, every bill you pay to a doctor or hospital, and every payment you make (or miss) on your mortgage, student loan or credit card bill. Imagine this company maintains a file on you containing all of this information going back five years. Imagine that this company uses your username and password to log into the online account you maintain with your bank and updates that file multiple times a day to stay up to date on every financial move you make.

2. Imagine this company is not your bank. Imagine that, as far as you know, you never provided your username and password to this company or otherwise authorized it to access your online accounts. Imagine you never heard of this company at all.

3. That company exists. It is called Plaid. And this is exactly what it does.

4. Plaid is one of the most successful tech startups in the financial technology, or "fintech," industry. It is perhaps the biggest tech company you've never heard of.

5. In January 2020, VISA purchased Plaid for $5.3 billion based, in part, on the "immense" universe of consumer data that Plaid has compiled, including years of highly detailed transaction history for as many as 200 million accounts from 11,000 financial institutions.

6. Plaid accumulated that data by serving as the "data plumbing" for popular mobile applications (or "apps") that allow users to transfer money to friends and businesses, such as Venmo, Stripe, and Cash App (f/k/a Square Cash), or make investments, like Robinhood. When a user of one of those apps tries to connect her bank account in order to fund such transfers, Plaid provides the link between the app and the bank. But when a user types in her username and password, Plaid does not simply pass the user along to the bank. Plaid keeps the credentials for itself and uses them to download incredibly detailed information on thousands of transactions, going back five years and going forward in perpetuity. The scope of the data Plaid gathers bears no relation to the service it provides, namely, connecting the user's bank account to the consumer-facing fintech app.

7. Plaid has succeeded in creating what it calls the greatest database of consumer transactional data in history through a decade-long campaign of lies and deceit. At the heart of

Plaid's scheme is a bait and switch—a sophisticated imitation of the logos and branding of major financial institutions, designed to fool users into thinking that they are interacting directly with their banks when in fact they are interacting only with Plaid. After Plaid has gathered reams of a user's sensitive personal data, Plaid aggregates the data with that of millions of other users, chops it up, and sells it to the highest bidder. These invasions of privacy are not incidental to an otherwise valid business model. Plaid's very purpose is to invade users' privacy for profit.

8. Plaid's conduct caused substantial harm to Plaintiff and Class Members, including by destroying their rights to indemnification for improper withdrawals from their bank accounts, by otherwise impairing the integrity of their data, and by damaging their dignitary rights.

9. Accordingly, Plaintiff brings this action on behalf of herself and a class of all others similarly situated for compensatory, punitive, and exemplary damages, as well as declaratory and injunctive relief requiring, among other things, that Plaid cease its illegal conduct and disgorge the credentials and data it illicitly obtained as well as profits it illicitly acquired.

II. JURISDICTION AND VENUE

10. 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.

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

12. 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.

13. 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.

14. 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

15. 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 Plaintiff's 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

16. **Plaintiff Logan Mitchell** is a citizen of California. She signed up to use the Venmo apps on or around August 15, 2015 via her mobile phone. She did so in order to send money to and receive money from friends, family and businesses. At the time, she was not aware of the existence or role of Plaid; does not recall providing her bank username and password to Plaid; and does not recall being prompted to read any privacy policy. At the time that Venmo prompted her to connect her bank account, she believed she was doing so through an official connection with her bank. She was unaware that she was providing her login credentials to Plaid, or that Plaid would then use those credentials to download (on a daily basis) her entire transactional history for all accounts associated with those credentials, or sell that data to third parties. Ms. Mitchell did not consent to Plaid engaging in any such conduct, did not receive an opportunity to opt out of such conduct and, if she knew then what she knows now, would not have used Plaid to connect her bank account to Venmo.

17. Ms. Mitchell signed up to use Cash App on or around September 20, 2015 via her mobile phone. She did so in order to send money to and receive money from friends, family and businesses. At the time, she was not aware of the existence or role of Plaid; does not recall providing her bank username and password to Plaid; and does not recall being prompted to read any privacy policy. At the time that Cash App prompted her to connect her bank account, she believed she was doing so through an official connection with her bank. She was unaware that she was providing her login credentials to Plaid, or that Plaid would then use those credentials to download (on a daily basis) her entire transactional history for all accounts associated with those credentials, or sell that

data to third parties. Ms. Mitchell did not consent to Plaid engaging in any such conduct, did not receive an opportunity to opt out of such conduct and, if she knew then what she knows now, would not have used Plaid to connect her bank account to Cash App.

18. Ms. Mitchell fears that Plaid's misconduct has increased her risk of identity theft and fraud.

19. Ms. Mitchell has used her bank's computer systems and servers to send and receive electronic communications related to her accounts, including checking balances, depositing checks, and making transfers.

20. **Defendant Plaid Inc.** is a financial technology company. Plaid is a Delaware corporation with its principal place of business at 85 Second Street, Suite 400, San Francisco, California 94105.

V. FACTUAL BACKGROUND

A. Founding of Plaid

21. In 2012, two former Bain & Co. consultants named William Hockey and Zach Perret began collaborating on a mobile app designed to help consumers track their finances. Looking back six years later, after Plaid had become a company valued at over a billion dollars, Hockey told a meeting of fintech software developers "how and why we started Plaid."[1] Initially, he said, he and Perret intended to help consumers "better control their finances," but soon realized, "[w]e weren't really consumer guys." Hockey and Perret determined that because "there wasn't a good way . . . to get consumers' transaction history, account data, or anything like that," they would instead develop Plaid as a "back-end, developer-focused infrastructure company." Hockey and Perret decided that the planning and financial management (or "PFM") tools they were building were less interesting to them than "decisioning analysis" and "risk modeling"—in other words, taking from users years of their transaction history and mining that data to make predictions about purchases

[1] *Deep Dive w/Plaid—William Hockey, Co-Founder & CTO*, Cambrian (Sept. 26, 2018), https://www.youtube.com/watch?v=9D5Rwt3DvGg. In his opening remarks, Hockey asked if anyone had heard of Plaid. Nearly everyone in the room, consisting of fintech software developers, raised their hands. This shows how well known Plaid is among a small coterie of experts, even while it remains almost completely anonymous to the millions of consumers whose data it collects.

they might make. As Hockey and Perret described it at an insular gathering of fintech software developers,[2] "[w]e wanted to know habits and how people were spending," and then "target people based on how they were spending." But Hockey and Perret learned that "[t]he problem with existing data sources is you can look back 30 days, 60 days, maybe 90 days. We wanted to look back 5 years." So they designed Plaid such that, as Hockey put it, "[t]he moment a user comes on we can look 2, 3, 4, 5 years back. So the amount of transactions we can actually hold is immense for an individual. That's 5-6,000 transactions." Thus, even with just "a couple of users," Hockey said, "the amount of transactions we can look at is immense and the potential applications are awesome."

22. Plaid's product offering thus evolved from a consumer-facing app aimed at helping users plan their financial lives to largely invisible plumbing designed to amass a huge mountain of data at consumers' expense. Even the goal of providing the infrastructure that connects users' financial accounts to fintech apps, which enabled Plaid to accumulate that mountain of sensitive user data in the first place, has since evolved to a new goal: mining that mountain of data for profit. Plaid's website reveals the shift in the company's focus. According to the "About Us" page on its website, Plaid "started out by building the technical infrastructure APIs that connect consumers, traditional financial institutions, and developers. Today, we add key insights to the data access we provide with our suite of analytics products."

23. After Plaid pivoted from its initial mission, the company developed relationships with some of the most popular fintech apps. This included apps that allow people to transfer money or make consumer purchases, such as Venmo, Square's Cash App and Stripe; buy and sell cryptocurrencies, such as Coinbase; or invest in equities, options and other investment assets, such as Robinhood (together, the "Participating Apps"). Plaid is not an app that a user downloads directly. It does not appear on the Apple or Android app stores that most mobile phone users visit to download apps. Instead, Plaid is embedded in the Participating Apps, adding a functionality that the Participating Apps don't provide themselves. Plaid persuaded the Participating Apps to allow Plaid to be the data plumbing connecting users to their bank accounts, thus enabling them to make

[2] *Zach Perret and William Hockey, Plaid.io // NYC Data Business Meetup // Feb 2013*, Data Driven NYC (Dec. 5, 2013), https://www.youtube.com/watch?v=_I8DRbFmLKM.

ACH transfers to and from those accounts using the apps.

24. By partnering with the Participating Apps, Plaid gained access to hundreds of millions of consumers. Venmo (now owned by PayPal) has over 52 million active user accounts; Coinbase reportedly has more than 30 million;[3] and Cash App reportedly has more than 24 million.[4] Stripe's payment service reportedly is used by millions of businesses, and thus a commensurate number of consumers.[5] Many of those users utilize Plaid to connect their bank accounts to the Participating Apps. Plaid itself claims that it connects to 11,000 financial institutions; that 1 in 4 Americans have provided their bank login credentials to Plaid; and that it has gathered data from and retains credentials for as many as 200 million distinct financial accounts.

25. Plaid now describes itself as an "infrastructure" company, but even that description conceals Plaid's true purpose: invading consumers' privacy for profit. In a 2019 interview, Perret revealed that the name Plaid refers to an algorithm he and Hockey devised to conduct "cross-user comparisons": comparing users' transaction patterns to those of other users against the backdrop of Plaid's database of merchants. The overlapping patterns resembled a crosshatch pattern—hence the name.[6]

B. Plaid Deliberately Undermines Industry Standard Security Protocols In Order to Trick Users Into Giving Plaid Their Bank Login Credentials

26. Plaid has acquired its mountain of consumer data by deceiving consumers into giving Plaid the key to their financial lives: their bank usernames and passwords.

27. Historically, in order to allow a third party access to a bank account, a user had to submit her bank routing and account numbers; transfer a small trial deposit (usually a few cents); and then return to the bank to verify the amount transferred.[7] This could take several days and, in

[3] *About Us*, Coinbase (last visited June 23, 2020), https://www.coinbase.com/about.

[4] Daniel Keyes, *Square's Cash App User Base Surges to a Massive 24 Million Monthly Active Customers*, Business Insider (Feb. 28, 2020), https://www.businessinsider.com/squares-cash-app-reached-24-million-users-and-monetization-surge-2020-2.

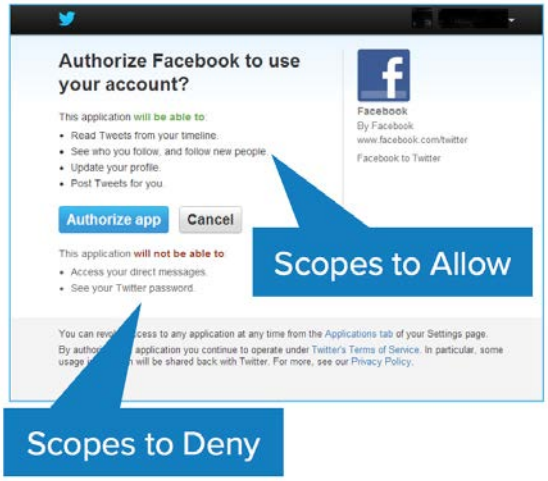
[5] *Customers*, Stripe (last visited June 23, 2020), https://www.stripe.com/customers.

[6] *Fireside Chat: Zach Perret, Founder & CEO of Plaid (FirstMark's Data Driven NYC)* at 10:45 to 11:45, Data Driven NYC (May 13, 2019), https://www.youtube.com/watch?v=sgnCs34mopw ("Perret Interview").

[7] *DEEP DIVE with Plaid: Fintech's Super-Connector*, FinTechtris (Oct. 24, 2018),

the fast moving world of fintech, that delay would cause many potential customers to abandon their adoption of a fintech app. In the terminology of the software world, this reduced new user conversions.

28. One alternative to this arduous process is **"OAuth."** Users are likely familiar with this procedure because it has become the industry-standard protocol for users who wish to grant a website or app permission to access certain information from another website or app. Crucially, OAuth "enables apps to obtain limited access (scopes) to a user's data without giving away a user's password." For instance, consider an example in which a user wishes to grant Facebook permission to access her Twitter account so that she can integrate her social media accounts together. Before she can do so, the user will be redirected from Facebook to Twitter, where she must login to ensure she is authorized to grant those permissions.[8] Then, a dialogue box pops up, asking which permissions she is granting and which she is denying. The dialogue box might look something like this:



[9]

29. In this example, note that the user grants Facebook permission to update her Twitter

---

https://www.fintechtris.com/blog/2018/10/20/plaid-fintech-super-connector.

[8] Redirection from the app the user is currently using to the app where it retains the data to which it is granting permission is a hallmark of OAuth. *See OAuth 2.0*, OAuth (last visited June 23, 2020), https://oauth.net/2/.

[9] *See* Matt Raible, *What the Heck is OAuth?*, Okta (June 21, 2017), https://developer.okta.com/blog/2017/06/21/what-the-heck-is-oauth.

profile and even post to the user's Twitter account ("This application will be able to: . . . Update your profile; Post Tweets for you"), but *denies* Facebook permission to see the user's Twitter password ("This application will not be able to: . . . See your Twitter password"). Instead, the user provides her Twitter username and password only to Twitter. Twitter then sends a "token" to Facebook, essentially confirming to Facebook that the user's login to Twitter was legitimate. Scopes are one of the "central components" and perhaps even "the first key aspect" of OAuth.

30. But as with the old-fashioned way of authorizing a bank account by providing account and routing numbers and waiting for a small deposit, OAuth purportedly undermines an app's user conversion rate. Because it requires a user to leave the app and be redirected to another app, OAuth supposedly drives consumers away who decide it isn't worth the trouble.

31. So Plaid devised an alternative to traditional bank verification or even OAuth: "Managed OAuth," which it also calls "Screenless Exchange," the technology underlying the "Plaid Link" software that Plaid embeds in each of the Participating Apps. Plaid co-founder Perret has described Managed OAuth as "kind of like OAuth, where the OAuth is embedded in the application. It's not technically OAuth, but it behaves very similarly."[10]

32. Plaid claims that Managed OAuth is "technically" different from OAuth in that it eliminates the need to redirect a user to her bank's website.[11] But there are several other important distinctions between industry-standard OAuth and Plaid's Managed OAuth. *First*, Plaid does not provide a clear dialogue box outlining the scopes of the permissions that the user is granting to Plaid or the permissions the user is denying to Plaid (indeed, the user has no option to deny Plaid any permissions at all).

33. *Second*, and more importantly, the core principle of OAuth—and what has made it the industry-standard authorization protocol—is that an app like Plaid can obtain limited access to

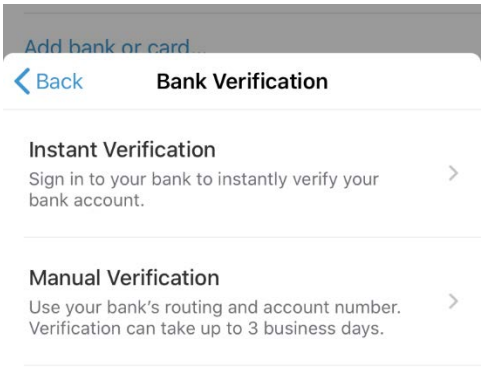
[10] Perret Interview at 17:30-17:45.May 13, 2019 interview with Zach Perret at Data Driven NYC event at 17:30-17:45, https://www.youtube.com/watch?v=sgnCs34mopw.

[11] Eric Showen, *Demystifying Screenless Exchange*, Fin (Nov. 15, 2016), https://fin.plaid.com/articles/demystifying-screenless-exchange/. ("Screenless Exchange combines the security advantages of OAuth—such as tokenization—with the design elements offered by solutions like Plaid. Specifically, Screenless Exchange is different because it allows a user to permission access to personal financial data without ever leaving the original app.")

a user's data *without accessing the user's password*. But Plaid designed Managed OAuth specifically to circumvent this precaution and to deceive users into giving up their bank usernames and passwords *to Plaid*. Plaid achieves this fraud by erecting a sophisticated edifice of deceit to trick users into thinking that they are logging into their financial institutions, when in fact they are turning over their credentials to Plaid.

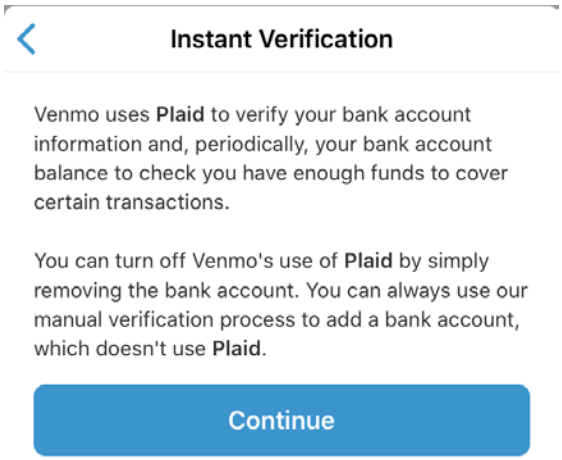
C. Plaid Deceives Users By Representing Itself To Be Their Financial Institutions

34. Consider the following hypothetical user experience of Plaid Link. A user downloads Venmo and creates an account, with the intent of sending money to a friend. Because it is her first time using the app, she has no balance in her Venmo account, and needs to connect her checking account in order to have funds to transfer. After clicking on "Add bank or card...," the user will see the below message pop up:



35. The user sees two options: "instant verification" or "manual verification." Manual verification refers to the process of using a bank's routing and account number and sending a small deposit. As the dialogue box indicates, this can take up to 3 business days.

36. If the user selects instant verification, Venmo will display the following dialogue box:



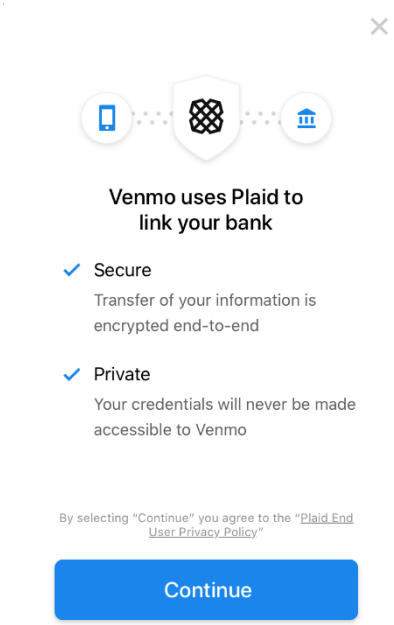
37. The dialogue box states, "Venmo uses Plaid to verify your bank account information and, periodically, your bank account balance to check you have enough funds to cover certain transactions." [12] The screen contains no description of what Plaid is or does, or even the fact that it is a distinct entity with no corporate affiliation with Venmo. It gives the misleading impression that Plaid is *only* collecting balance information. It does not disclose that Plaid will (as discussed below) download years of the user's transaction history for purposes entirely unrelated to connecting the user's bank account.

38. The dialogue box then states, "[y]ou can turn off Venmo's use of Plaid by simply removing the bank account." This statement misleads users by omitting the fact that once Plaid has obtained a user's credentials, removal of the bank account from Venmo has no effect on *Plaid's* retention and use of those credentials to collect, retain and sell the user's sensitive personal data

[12] Although the precise language that each Participating App uses to describe Plaid varies, Plaid has admitted that it plays a direct role in shaping those disclosures. *See* Perret Interview at 25:45-26:10 ("[O]ur customers are the ones that build the consumer apps. But there are certain elements of the consumer experience that are really important, such as making sure that a consumer understands data privacy. Where it's going, how it's going.") But in reality, Plaid either negligently fails to exercise this oversight or willfully sanctions the Participating Apps' failure to make adequate disclosures. For instance, if a user is attempting to link her bank account to Cash App, she will not even see the messages like the ones in the Venmo dialogue boxes described here. Instead, she proceeds directly to the Plaid Link iframe requesting user credentials as displayed in ¶50. Whether in Venmo (with its minimal and misleading disclosures), Cash (which makes no reference to Plaid at all) or otherwise, at no time are users of the Participating Apps informed in the app that Plaid will take their bank login credentials, retain them, and use them to collect extraordinarily detailed data about their financial lives, going back five years and going forward in perpetuity.

going forward.

39. If the user clicks "continue," a dialogue box comes up that indicates that use of Plaid is both "Secure" and "Private":



40. These representations are false.

41. *First*, the transfer of information is not **secure**. Plaid sends login credentials in plain text under only a single level of encryption. This leaves the credentials open to interception by a hacker with even a minimal level of experience. Further, after Plaid has collected and retained a user's information, including sensitive personal data, Plaid packages it into various products that it sells to the Participating Apps and other third parties. Plaid exercises no control or oversight over those third parties after it has sold it. Although it requires such customers to "handle End User Data securely" and adhere to best practices, Plaid has no enforcement or tracking mechanisms in place to ensure that developers do so.

42. The statement about the security of Plaid is not only false but also misleading. By stating that a user's information is encrypted end-to-end, Plaid gives the user the false impression that no entity other than Venmo and her bank will be able to access the user's bank balances, let alone the vast quantity of other sensitive personal data that Plaid collects. In fact, Plaid obtains this

data for use by itself and its third party customers.

43. *Second*, the transfer of information is not **private**. Plaid deceives the user into thinking that she is providing credentials only to her bank, using Plaid merely as a link. But it is misleading to say that the user's credentials will never be made accessible to Venmo. The user's credentials are made accessible to *Plaid*, which keeps the credentials for itself, using them to extract reams of sensitive personal data. Further, even if Venmo never obtains the user's credentials, Venmo may later obtain the data that the credentials protect—after Plaid has packaged it into analytics products that Plaid sells to the Participating Apps and others, as discussed below.

44. At the bottom of the dialogue box reproduced in ¶ 13 is a large blue button labeled "Continue." Above that, in small gray print is the language, "By selecting 'Continue' you agree to the 'Plaid End User Privacy Policy.'" That text is deemphasized in several ways. For instance, the text is smaller than other text on the screen and it appears in a light gray color that is more difficult to read than the other text on the screen. Although that text is underlined,[13] it does not appear in the blue color normally indicating a hyperlink. A user would not know that this text contains a link to Plaid's privacy policy unless she were to actually click on it. Nothing else on the screen directs the user to do so. The screen contains no requirement that the user *must* review (or even scroll through) the privacy policy before clicking "Continue."

45. This disclosure is known in the tech world as a "fine-print click-through" disclosure. This disclosure is inadequate to put a user on actual or constructive notice that if she proceeds, Plaid will gather information on every financial transaction she has made going back five years and going forward in perpetuity.[14] Plaid itself has admitted that such disclosures are inadequate. In a 2019 letter to the United States Senate Committee on Banking, Housing, and Urban Affairs, Plaid wrote, "[a]ffirmative 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

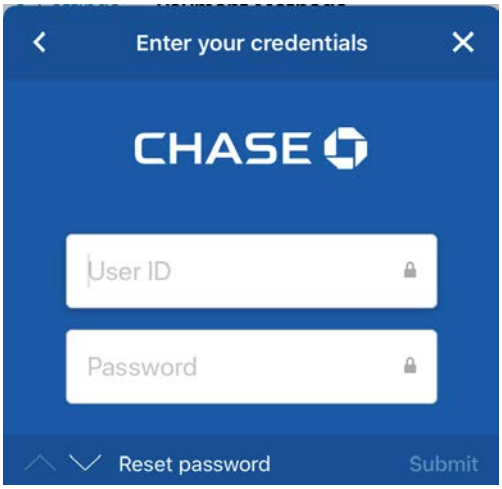
[13] The underlining is a recent addition that was not present as recently as a few months ago.

[14] As described more fully below, even if a user realizes that the gray language contained a hyperlink to the Privacy Policy, clicked through to that policy and reviewed it—as few if any users actually do—the Privacy Policy is riddled with so many misrepresentations and omissions that any consent to that Policy is invalid.

relationship with. To do otherwise would breach the trust consumers place in fintech providers."[15] Yet, as discussed below, Plaid *does* sell Plaintiff and Class Members' data—in aggregated form and otherwise—to the Participating Apps and other third party customers, despite the fact that Plaintiff and Class Members never consented to such sale of their data.

46. After the user clicks "continue," the app asks a user to "select your bank" from a list of approximately 16 of the nation's largest financial institutions. After selecting a bank, the screen on the app appears to slide to the left, mimicking the visual a user would see if the app redirected her to her bank's website.

47. Plaid designed the next steps of the process with the explicit intent of deceiving the user into thinking that she is in the secure environment of her trusted financial institution. Plaid Link presents the user with a login screen that mimics the look and feel of the user's bank, including by imitating its distinctive color scheme, font and logo. For example, if the user selects Chase, she will be directed to a login screen as depicted in this screenshot:



48. This interface features the word "Chase" in the bank's characteristic font; the Chase logo; and a background color in Chase's distinct navy blue. The same is true for Bank of America, Wells Fargo, Citibank, and thousands of other financial institutions.

49. Plaid has designed this entire process—including the "sliding" animation as well as

[15] *See* John Pitts, Plaid Submission to the U.S. Senate Committee on Banking, Housing and Urban Affairs (Mar. 15, 2019), *available at* https://www.banking.senate.gov/imo/media/doc/Data%20Submission_Plaid1.pdf.

the look and feel of the page asking for input of credentials—to mislead the user into thinking that she is being redirected to her bank's website, as would happen if Plaid deployed a true OAuth procedure. Plaid deliberately creates the false impression that the user is sharing her credentials only with her bank directly. In fact, the user has never left the Plaid Link interface within the Participating App and is sharing her login credentials with Plaid—not just temporarily and for the purposes of connecting her account but permanently and for whatever purposes Plaid chooses.

50. Plaid has admitted and even boasted that it designed its interface to give the user the false impression that she is dealing directly with her bank. In April 2016, a Plaid engineer bragged that Plaid had "completely optimized our drop-in module used for onboarding bank accounts."[16] Plaid attributed this success to its use of "design elements" that mirror the "look and feel of permissioning access" for the financial institutions, thus "increasing user conversion."[17] Plaid has admitted that it designed this approach to give users "a greater sense of security and familiarity."[18]

51. Various members of the developer community—including members of Plaid's own team—have called out the company for this misleading conduct. In late 2018, a poster on a now-deleted thread on the developer website GitHub called out the fact that a third party website was using a Plaid iframe to "render[] my bank's logo to fool me into thinking I'm accessing my bank's site."[19] Plaid engineer Michael Kelly responded:

> [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 [sic] 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

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

[17] Shown, *supra* n. 11.

[18] See Baker Shogry, *Improving Search for 9,600+ Banks*, Plaid (Dec. 13, 2017), https://blog.plaid.com/improved-search/ ("This means you'll see logos and brand colors for even more institutions in Link so that end-users feel a greater sense of security and familiarity when they recognize their institution's look-and-feel.").

[19] *Privacy/Security Concerns* #68, GitHub (Feb. 11, 2016), http://web.archive.org/web/20190415103059/https:/github.com/plaid/link/issues/68.

> security we provide, banks protect their users from credential-based attacks via multi factor authentication.

Kelly did not deny that Plaid was impersonating major financial institutions, or that others might try to use Plaid's code to do the same. Indeed, he indicated Plaid's awareness that precisely that kind of malicious conduct does take place.

52. In May 2018, a poster to the site Y Combinator Hacker News warned others against using the stock-trading app Robinhood because of concerns about Plaid: "I would really caution connecting your bank account through Plaid on RH. 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." The poster was right that someone was collecting his entire bank account transaction history, but he was mistaken that the malfeasor was Robinhood rather than Plaid. Plaid co-founder Hockey responded, "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."[20] Notably, Hockey did not deny that *Plaid* was collecting Plaid's full transaction history; only that Robinhood was not. This deflection echoes the language noted above in the Venmo disclosure, "[y]our credentials will never be made accessible *to Venmo*." The credentials are, of course, made accessible to Plaid. This linguistic sleight of hand does not justify Plaid's deceitful conduct, particularly where that conduct leads to invasions of privacy on a massive scale.

53. Any consent that Plaid claims to have obtained from Plaintiff and Class Members is further called into question by the fact that most consumers do not recognize that Plaid is an entity distinct from the Participating App that they are using, or even—as Plaid boasts—that Plaid exists at all. Co-Founder Hockey has said in interviews that "most people will never know we exist."[21]

[20] *See Stock-Trading App Robinhood Was Rejected by 75 Investors*, Y Combinator Hacker News (May 13, 2018), https://news.ycombinator.com/item?id=17060034.

[21] *See* Nick Sommariva, EmoryWire (Aug. 2013), http://www.alumni.emory.edu/emorywire/issues/2013/august/of_interest/story_1/index.html#.XksqMxNKjQg.

Perret has stated, "we don't need every consumer to know what Plaid is."[22] One of Plaid's investors at Goldman Sachs Investment Partners told CNBC, "Plaid has quietly created a very big infrastructure without the consumer knowing that they're powering it."[23]

54. If consumers don't know that Plaid exists, they certainly cannot consent to Plaid taking their data. Plaid intentionally designs the software interface that a user sees when connecting her bank account to a Participating App to ensure that the user does not receive actual or constructive notice of Plaid's conduct—including that Plaid is collecting the user's login credentials and then using them to collect, retain and sell vast quantities of her sensitive personal data. Plaid knows that if its users *were* on notice of the massive invasions of privacy in which Plaid engages, it would never secure consent of any kind.

D. Plaid Gathers Data Far Beyond What it Needs for the Services It Provides

55. In response to a 2017 Request for Information from the Consumer Financial Protection Bureau (the "CFPB RFI"), Plaid wrote, "[m]inimization is a key principle that should govern data use; it is the concept that permissioned parties should collect only a rational amount of data to service a product or service, and store such data for the necessary amount of time. Data 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."

56. In practice, Plaid departs from every word of this statement.

57. First, **Plaid collects far more data than it needs**. Plaid does not collect only a rational amount of data to support the service it provides to Plaintiff and Class Members, namely, linking their bank accounts to the Participating Apps. Instead, from "[t]he moment a user comes on" to Plaid's system, Plaid looks back 5 years into their financial histories and gathers information regarding "5-6,000 transactions." In Plaid's own words, "the amount of transactions [Plaid] can

[22] *See* Feb. 2019 interview with Zach Perret at 19:08 to 19:37; Louise Lee, *the Plaid Story: Integrating with 10,000 Institutions. On the Way to a $5 Billion Acquisition*, SaaStr (Jan. 14, 2020), https://www.saastr.com/build-a-platform-ecosystem/.

[23] *See* Kate Rooney, *Meet the Start-Up You've Never Heard of that Powers Venmo, Robinhood, and Other Big Consumer Apps*, CNBC (Oct. 4, 2018), https://www.cnbc.com/2018/10/04/meet-the-startup-that-powers-venmo-robinhood-and-other-big-apps.html (emphasis added).

look at is immense." In job postings on the influential software developer forum Y Combinator Hacker News, co-founders Hockey and Perret have repeatedly described Plaid as "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."[24] The data Plaid collects data extend into every corner of users' lives, including their spending and borrowing related to health care, education, transportation, political contributions, dining, entertainment, and other habits, as well as investment and retirement savings.

58. Plaid has claimed that it is entitled to this data under users' assignments to Plaid of their rights under the Dodd-Frank Act. *See* Perret Interview at 23:00-23:30 ("In the early days, there's a provision of Dodd-Frank that consumers must have access to a digital copy of their financial data. We operated under this principle where consumers assigned us that and we then went and collected the data from the bank."). Nowhere in Plaid's statements to users of the Participating Apps does it disclose that it is gathering data pursuant to Dodd-Frank or that it is asking users to assign those rights to Plaid.

59. Because it is largely automated, Plaid's collection of sensitive personal data is indiscriminate. It gathers financial data regardless of the protections, described below, that statutes and public policy ascribe to users' financial information. It gathers health-related data regardless of the Health Insurance Portability and Accountability Act ("HIPAA"). And it gathers all of this information regardless of the age of the account holder, thus gathering extensive information about minors.[25] The scope of the data that Plaid collects is utterly disproportionate to the services it provides to users of the Participating Apps and is not routine commercial behavior.

60. Second, **Plaid retains user data for far longer than necessary and re-collects it**

[24] *Plaid Technologies – plaid.io*, Y Combinator Hacker News (Feb. 1, 2013), https://news.ycombinator.com/item?id=5151764; *Plaid Technologies – http://plaid.io/jobs*, Y Combinator Hacker News (Mar. 1, 2013). https://news.ycombinator.com/item?id=5304472; *Ask HN: Who is Hiring? (July 2015)*, Y Combinator Hacker News (July 1, 2015) https://news.ycombinator.com/item?id=9812245.

[25] Even if the user of the Participating App is an adult, if that adult uses the same login credentials it provides to Plaid to access the accounts of a minor for whom it acts as a custodian, Plaid will access, collect, retain and sell the data from that account.

far more often than necessary. Plaid stores the data that it collects for far longer than is necessary to connect user bank accounts to the Participating Apps. Plaid collects this data not only at the time that users of the Participating Apps connect their financial accounts, but on a constant, rolling basis and then stores it indefinitely. According to Plaid's Head of Engineering, Plaid is "effectively caching" the banking data.[26] Plaid "update[s] a user[']s account at set intervals throughout the day, independent of how many times a client calls the /connect endpoint"—in other words, regardless of the last time the user actually used the Participating App.[27] This can happen as often as multiple times *per day*, or every 4-6 hours, going forward in perpetuity.

61. Third, **Plaid is not transparent about the data it collects**. As detailed throughout this Complaint, Plaid acquires data from Plaintiff and Class Members only through an elaborate web of lies, fraud and deceit that it has erected with the express intention of extracting from them their sensitive personal data. It does not disclose to users in plain English the data it accesses or the fact that it collects, retains and sells it.

E. Plaid Sells User Data, Despite Its Explicit Promise to Not Do So

62. In the privacy overview on Plaid's website, it claims, "we never sell your data." This is false.

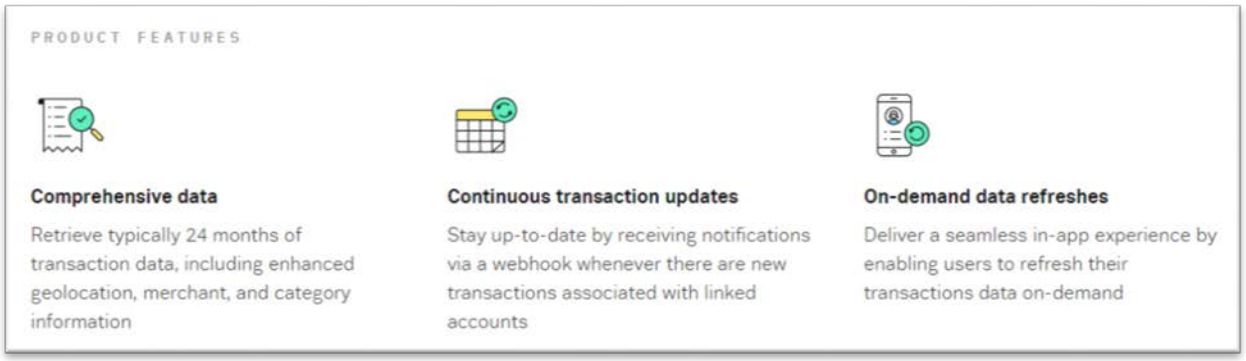
63. In fact, Plaid *does* sell user data. The Plaid website admits that the company is pivoting from what its co-founders have called Phase 1—building its "immense" database of consumer data—to Phase 2: "add[ing] key insights to the data access we provide with our suite of analytics products."[28]

[26] *See Plaid: Banking API Platform with Jean-Denis Greze*, Software Engineering Daily (Dec. 13, 2018), https://softwareengineeringdaily.com/2018/12/13/plaid-banking-api-platform-with-jean-denis-greze/.

[27] *See Plaid Legacy API*, Plaid (last visited June 23, 2020), https://plaid.com/docs/legacy/api/.

[28] *See Our Vision*, Plaid (last visited June 23, 2020), https://plaid.com/company/. *See also* Perret Interview at 12:30-13:15 ("We're continuing to do more analytics on top of the data. It's an immense pile of data that we have."); 14:21 to 14:26.

64. Plaid could not sell those analytics products without the mountain of consumers' private data that it has amassed. And the data up for grabs is extensive. For example, Plaid advertises that it offers customers access to "detailed transaction history," including the following product features:



The first two categories are aimed at third parties, not users. The first category suggests that while Plaid collects as much as five years of user data, it offers customers the opportunity to "[r]etrieve typically 24 months of transaction data, including enhanced geolocation, merchant, and category information." The second category highlights Plaid's ability to constantly ping Plaintiff and Class Members' financial accounts on an ongoing basis by offering, "[c]ontinuous transaction updates: Stay up-to-date by receiving notifications via a webhook whenever there are new transactions associated with linked accounts." In sum, Plaid can only offer these services because of the enormous amount of data that Plaid takes from users and then updates even more often than once per day.

65. 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."[29] Plaid investor Goldman Sachs has explained that Plaid has developed a "sustainable moat or advantage" against its competitors because the Participating Apps rely upon Plaid to understand their own users' behavior.[30]

[29] *See Ask HN: What Is the Most Unethical Thing You've Done As a Programmer?*, Y Combinator Hacker News (Aug. 5, 2018) https://news.ycombinator.com/item?id=17692291.

[30] *See* Rooney, *supra* n.23.

F. Plaid's Privacy Policy is Misleading

66. In the unlikely event that a user clicks through to review Plaid's privacy policy—which the vast majority of users do not, because nothing requires them to do so—that policy fails to place Plaintiff and Class Members on actual or constructive notice of the outrageous invasions of privacy in which Plaid engages. As a result, any consent to that Policy is not only questionable but invalid.

67. The Privacy Policy begins with the phrase, "Privacy and security are very important to us at Plaid." It continues, "[o]ur goal with this Policy is to provide a simple and straightforward explanation of what information Plaid collects from and about end users . . . and how we use and share that information. We value transparency and want to provide you with a clear and concise description of how we treat your End User Information."[31] These statements are false and misleading.[32]

68. In California, multiple statutes govern the disclosures that a privacy policy like Plaid's must contain. The California Consumer Privacy Act (the "CCPA") requires that any "business that collects a consumer's personal information" must "inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section." Cal. Civ. Code § 1798.100(b). Similarly, the California Online Privacy Protection Act ("CalOPPA") requires that "[a]n operator of

[31] *Legal*, Plaid (last visited June 23, 2020), https://plaid.com/legal/.

[32] In addition to its formal privacy policy, Plaid's website also contains a page offering an overview of its approach to privacy that is briefer and written in less legal language. *See Privacy*, Plaid (last visited June 23, 2020), https://plaid.com/overview-privacy/. This statement also contains misrepresentations and omissions of material fact. For instance, the page states, "When you connect a financial account to an app or service using Plaid, you allow us to access your account data so that we can deliver it to the apps you want to use." It does not state that Plaid also retains this data for itself, nor does it disclose that the "account data" it captures is deeply invasive details of every financial transaction from the past five years. The page also states, "We're committed to handling your data with the utmost care and respect for your privacy. It's why we never sell your data." As noted herein, Plaid does sell user data and products based off of user data.

a[n] . . . online service that collects personally identifiable information through the Internet about individual consumers" must "[i]dentify the categories of personally identifiable information that the operator collects . . . about individual consumers who use or visit its . . online service and the categories of third-party persons or entities with whom the operator may share that personally identifiable information." Cal. Bus. & Prof. Code § 22575.

69. Plaid violates these statutes because the vague descriptions in its Privacy Policy do not put consumers on notice of the full scope and extent of its data practices.

70. *First*, Plaid's Privacy Policy omits material facts: Plaid *does not disclose* that rather than merely providing a link to Plaintiff and Class Members' financial institutions, as it suggests, Plaid in fact collects and retains users' bank login information for its own purposes. Plaid *does not disclose* that it uses those credentials to access Plaintiff and Class Members' accounts. Plaid *does not disclose* any information about the temporal scope of the data it collects, including that Plaid accesses at least five years' worth of transaction history. Plaid *does not disclose* that it retains Plaintiff and Class Members' login credentials and data indefinitely. Plaid *does not disclose* that it continues to access Plaintiff and Class Members' accounts and scrapes their updated transaction history multiple times per day, going forward in perpetuity—regardless of how often the user uses the Participating App, including if she stopped using it entirely or never used it at all. Plaid *does not disclose* that it uses, sells and otherwise benefits from the data that it collects, including to the Participating Apps and others. Plaid *does not disclose* that after it sells Plaintiff and Class Members' data to third parties, it exercises no oversight or control over how that data is stored, used, or secured. Plaid *does not disclose* that by removing Plaintiff and Class Members' data from the secure banking environment, it is destroying their rights to indemnification and other important rights and protections.

71. *Second*, the disclosures that Plaid does make are too vague to be sufficient. The Privacy Policy gives the user the false impression that it collects only the data necessary to link her account to a Participating App, because it emphasizes basic information such as the user's account number and balance.

72. *Third*, Plaid's Privacy Policy states that the information it gathers "varies depending

on the specific Plaid services developers use to power their applications, as well as the information made available by those providers." In fact, Plaid's collection of user data has no relationship to the Plaid services that developers use. Once Plaid gains a user's bank login credentials, it gathers *all* available transaction history and other data from *all* accounts linked with those credentials, regardless of whether the user has sought to connect a particular account to the Participating App and regardless of any relationship between the data Plaid collects and the service it is providing. Even the entry level analytics product that Plaid offers for sale to developers provides two years of user transaction history.

73. *Fourth*, under the heading "How We Use Your Information," Plaid's Privacy Policy lists seven highly vague purposes, such as "To operate, provide and maintain our services" and "To develop new services." This gives the misleading impression that Plaid is gathering the data for the benefit of consumers, i.e., to improve users' experience and provide them with additional and superior services. In fact, as Plaid's co-founders have admitted, they are "not consumer guys." The data that Plaid collects, for the most part, has nothing to do with the services it provides to users, but is geared towards supporting the analytics products that it sells to third parties.

G. Plaid's Public Statements Are Misleading

74. In addition to the misstatements and omissions in Plaid's Privacy Policy, Plaid and its co-founders have repeatedly made statements in public that give the impression that it operates in the best interest of consumers and is committed to the security and privacy of their data. These statements are false.

75. In February 2019, the Senate Banking Committee sought feedback from stakeholders regarding "the collection, use and protection of sensitive information by financial regulators and private companies." Plaid's response described an aspirational, consumer-centric view of its business that completely misrepresents its actual practices.

76. In its letter, Plaid claimed that it "help[s] 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."[33] Plaid knows well that Plaid does not allow consumers to share their data only with companies they select, since Plaid itself collects, retains and sells consumers' data; of course, a consumer cannot "select" to share her data with a company like Plaid if she does not know it exists. Likewise, Plaid knows that the company's model does not permit consumers to "control what they do with their data" since, once Plaid takes it, consumers have *no* control over what Plaid does with it. And even Plaid exercises no control or oversight over user data after it sells it.

77. Plaid's letter to the Senate Banking Committee also states, "[a]t 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." As discussed above, Plaid's permissioning protocol departs from the industry-standard permissioning protocol, OAuth, in material ways, including because it deceives users into providing their login credentials directly to Plaid and because it fails to sufficiently disclose or cabin the scopes of those permissions.

78. Plaid's letter to the Senate Banking Committee also states, "consumer permission should be tied to the services the consumer requests or purposes for which they are specifically informed when they grant access." Yet as this Complaint makes clear, Plaid's collection, retention and sale of Plaintiff and Class Members' sensitive personal data are completely out of proportion to the service Plaid supposedly provides: connecting bank accounts to the Participating Apps.

79. In various other statements, Plaid and its co-founders have expressed their commitment to consumer welfare, even as Plaid's conduct consistently belies those platitudes. For instance, Plaid's website states that it designed its products to "help users manage, budget and make sense of their money." It describes its "vision" as "democratizing financial services through technology," and that its "mission is to improve people's lives by delivering access to the financial

[33] *See Crapo, Brown Invite Feedback on Data Privacy, Protection and Collection*, U.S. Senate Committee on Banking Housing, and Urban Affairs (Feb. 13, 2019), https://www.banking.senate.gov/newsroom/majority/crapo-brown-invite-feedback-on-data-privacy-protection-and-collection.

system." It states that "[b]y delivering access to high-quality, usable financial account data that we've translated and standardized, we enable developers to focus on building experiences that benefit you."[34] Co-founder Perret told an interviewer, "[o]f course, we're doing things only that benefit the consumer. . . . It's a lot of data but we need to make sure that the products we're building are in the consumer's best interest."[35] Perret has also said that 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 [there]."[36]

80. If Plaid were truly committed to building products that are in consumer's best interests, it could apply the same standards in the United States that it applies in Europe. On September 14, 2019, the European Union's new privacy rule, Payment Services Directive No. 2 ("PSD2"), became effective. One key element of the new regulation is that a company like Plaid must *not* gather users' credentials or accumulate years of their transactional history. In order to comply with this policy, Plaid implemented a new approach for European users: "Plaid's PSD2-compliant European integrations use a protocol called OAuth 2.0 (Open Authorization) that allows users to share their financial data *without giving Plaid access to their bank login credentials*. Users can then revoke access to their data at any time via their bank's website, or extend access via Link update mode." Plaid co-founder Perret has stated that PSD2 "is good for consumers, so we're excited."[37] If Plaid were in fact committed to acting in the interest of consumers in the United States, it would implement OAuth 2.0 in the United States, regardless of whether it is required by law to do so. Instead, Plaid has continued to pursue its strategy of collecting Plaintiff and Class Members' login credentials and data through a sophisticated system of fraud and deceit.

[34] *See Legal*, supra n. 31.

[35] Perret Interview at 13:18 to 13:34.

[36] Perret Interview at 21:38 to 26:11. *See also id.* at 29:35-30:00 ("We don't directly touch consumers. But our goal is to create an ecosystem where the consumer wins. . . . It's about the end customer that is getting the value out of financial services.").

[37] Perret Interview at 30:50 to 31:20.

H. Plaid Violates Statutory Standards for Treatment of Financial Data

81. The Graham Leach Bliley Act (the "GLBA") and the regulations promulgated thereunder impose strict requirements on financial institutions regarding their treatment of consumers' private financial data and the disclosure of their policies regarding the same. Plaid is a financial institution subject to those regulations, which include the Privacy of Consumer Financial Information regulations (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. Plaid acknowledged as much in its February 2017 responses to the CFPB RFI, in which it conceded that "[a]n existing legal framework – the Gramm-Leach-Bliley Act (GLBA) – governs the proper disclosure and use of consumer financial data. Ecosystem participants – both traditional institutions and newer digital players – should abide by this framework."[38] Plaid also admits that the data it sells or otherwise transfers to Participating Apps and other third parties is subject to the GLBA's "Safeguards Rule" (16 C.F.R. Part 314).

82. This regulatory scheme has clear requirements for applicable privacy policies. Under those rules, a financial institution "must provide a clear and conspicuous notice that accurately reflects [its] privacy policies and practices." 16 CFR 313.4. 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. "Clear and conspicuous means that a notice is reasonably 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). Ways a company can call attention to its privacy policy include "[using] a plain-language heading" (16 CFR §313.3(b)(2)(ii)(A); "[using] a typeface and type size that are easy to read" (16 C.F.R.§ 313.3(b)(2)(ii)(B)); (c) "[using] boldface or italics for key words" (16 C.F.R. § 313.3(b)(2)(ii)(D)); or (d) "[using] distinctive type size, style, and graphic devices, such as shading or sidebars," when combining its notice with other

[38] Response by Plaid to CFPB's Consumer Data Access RFI (Feb. 21, 2017), *available at* https://plaid.com/documents/Plaid-Consumer-Data-Access-RFI-Technical-Policy-Response.pdf. *See also Legal*, Plaid (last visited June 23, 2020), https://web.archive.org/web/20160920005638/https://plaid.com/legal/ (instructing developers that their "product must maintain a clear and conspicuous link in its privacy policy to Plaid's Privacy Policy").

information. 16 C.F.R. § 313.3(b)(2)(ii)(E). A company must ensure that "other elements on the web site (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice." 16 CFR §313(b)(2)(iii). The notice should appear in a place that users "frequently access." 16 CFR §313.3(b)(2)(iii)(A), (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.

83. California's Financial Information Privacy Act (CalFIPA) likewise requires that the language in privacy policies be "designed to call attention to the nature and significance of the information" therein, use "short explanatory sentences," and "avoid[] explanations that are imprecise or readily subject to different interpretations." Cal. Fin. Code §4053(d)(1). The text must be no smaller than 10-point type and "use[] boldface or italics for key words." *Id.* In passing CalFIPA, the California legislature explicitly provided that its intent was "to afford persons greater privacy protections than those provided in . . . the federal Gramm-Leach-Bliley Act, and that this division be interpreted to be consistent with that purpose." Cal. Fin. Code § 4051.

84. Another California statute, CalOPPA, also requires that an operator of any online service, as defined therein, "conspicuously post" its privacy policy. Cal. Bus. & Prof. Code §22575. It specifically defines "conspicuously post" to require a text hyperlink to the policy that includes the word "privacy"; is "written in capital letters equal to or greater in size than the surrounding text"; "is written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language." Cal. Bus. Prof. Code § 22577(b).

85. Both GLBA and CalFIPA require that privacy policies provide consumers with an opportunity to opt out of the sharing of their personal data. 16 C.F.R. § 313.10; Cal. Fin. Code. §4053(d)(2).

86. Plaid's Privacy Policy fell short of these requirements in at least 3 ways.

87. *First*, Plaid's Privacy Policy is not clear and conspicuous and is not provided such that Plaintiff or Class Members could reasonably be expected to receive actual notice of its terms. In some iterations of the Plaid Link software, such as the one embedded in Cash App, there is no reference to Plaid whatsoever—let alone a link to its privacy policy or a disclosure that Plaid is collecting and retaining a user's login credentials. In Venmo, there is no notice of Plaid's Privacy Policy at all, other than the small, gray hyperlink in the Plaid Link dialogue box. That language does not appear in a typeface or type size that is easy to read and is not designed to call attention to the nature and significance of the information in the notice. To the contrary, it is deliberately hidden. Rather than using a distinctive type size, style or graphic device to draw attention *to* the link to the Privacy Policy, the link appears in a gray font smaller than all other text on the dialogue box. If anything, the dialogue box emphasizes the misleading statements that use of Plaid is "secure" and "private" to distract attention from the notice, rather than ensuring that such statements would *not* distract attention from the notice. Finally, the hyperlink does not appear on a page that users frequently access; it appears only upon initial sign up.

88. *Second*, Plaid's Privacy Policy does not accurately reflect its privacy policies and practices. Neither the Venmo dialogue box containing the hyperlink nor the Privacy Policy itself sufficiently emphasize—or even disclose—material facts that would be essential to any meaningful consent to the Privacy Policy, as detailed above. In the Privacy Policy, the vague description of each category of data Plaid collects and its policies and practices regarding storage and use of that data violate the rule that Plaid must "[a]void explanations that are imprecise and readily subject to different interpretations." 16 C.F.R. § 313.3(b)(2)(i)(F).

89. *Third*, Plaid's Privacy Policy provides an insufficient opportunity to opt out, including because it fails to use the heading "Restrict Information Sharing With Other Companies We Do Business With To Provide Financial Products And Services." Cal. Fin. Code 4053 (d)(1)(A).

90. In addition to itself being a financial institution governed by the GLBA and CalFIPA, Plaid also received data from other financial institutions. As such, it violated the following CalFIPA provision as well:

> An entity that receives nonpublic personal information pursuant to any exception set forth in Section 4056 shall not use or disclose the information except in the ordinary course of business *to carry out the activity covered by the exception under which the information was received.*

Cal. Fin. Code § 4053.5 (emphasis added).

91. One of the exceptions noted in Section 4056 allows sharing of nonpublic personal information "with the consent or at the direction of the consumer." Cal. Fin. Code. § 4056. Plaintiff and Class Members did not consent to or direct the release of their sensitive nonpublic personal information for the reasons described herein. But even if they did, Section 4053.5 still provides that an entity like Plaid can *only* use such information to carry out the activity *for which the user provided consent*. Plaid's use of the data for a myriad of reasons that extend far beyond connection of users' Participating App accounts to their bank accounts violates this statutory protection.

I. Government and Industry Leaders Agree that Plaid's Conduct Is Wrong, Risky, Dangerous and Bad for Consumers

92. Government and industry leaders agree that Plaid's conduct runs afoul of basic standards of decency and proper treatment of consumer data.

93. The Consumer Financial Protection Bureau has stated that data services like Plaid should not "require consumers to share their account credentials with third parties"—i.e., anyone other than the user or the bank. Of course, Plaid does exactly that.[39]

94. Likewise, the CFPB's October 2017 Consumer Protection Principles provide that the data practices of a company like Plaid 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." Plaid's disclosures were not full and effective, as described above. Plaid's data practices were not understood by Plaintiff and Class Members, are overly broad, and are not consistent with consumers' reasonable expectations, since they are wildly out of proportion to what is actually necessary to link a bank account to a Participating App.

[39] *See* Response by Plaid to CFPB's Consumer Data Access RFI, *supra* n. 38, at 12.

95. The Consumer Protection Principles also provide that data access terms must address "access frequency, data scope, and retention period." The Privacy Policy egregiously omits any mention of how often it accesses consumers' data, how much data it gathers and how long it keeps it—perhaps because consumers would be outraged to learn that *more than once a day*, Plaid gathers their *entire transaction history* and retains that information *indefinitely*.

96. The Consumer Protection Principles also provide that 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."[40] Plaid does not disclose this information.

97. Major financial institutions and their trade associations have also voiced concerns. In April 2016, JPMorgan CEO Jamie Dimon said the bank is "extremely concerned" about "outside parties," including "aggregators" (like Plaid), for three reasons: first, "[f]ar more information is taken than the third party needs in order to do its job"; second, "[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 third, "[o]ften 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."[41] Dimon recommended that users *not* share their login credentials with third parties like Plaid, in part to avoid loss of important indemnification rights: "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 customer's account, the customer, not the bank, is responsible for any loss. . . . This lack of clarity and transparency isn't fair or right." JPMorgan hit the nail on the head in identifying the egregious invasions of privacy that are not simply incidental to Plaid's business, but lie at the heart of it.

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

[41] *See Letter from JPMorgan Chase to Shareholders* (Apr. 6, 2016), *available at* https://www.jpmorganchase.com/corporate/annual-report/2015/.

98. In 2017, the American Bankers Association ("ABA") wrote to the CFPB to express similar concerns. The ABA stated that "few consumers appreciate the risks presented when they provide access to financial account data to non-bank fintech companies," including the risk of removing such data from the secure bank environment; that "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"; that aggregators like Plaid make "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"; and that "[c]onsumers assume that data aggregators take only the data needed to provide the service requested," but in reality, "too often it is not the case."

99. Plaid boasts that many large banks are now its primary customers. But some banks have refused to allow Plaid to collect, retain and sell their customer's data. PNC Bank blocked Plaid and other data aggregators from accessing customer accounts after it identified attempts to circumvent technical or code-based barriers PNC had erected.[42] As PNC's head of retail banking told the Wall Street Journal, "When aggregators access account numbers, many store them indefinitely, often unbeknownst to customers. This puts customers and their money at risk." The same PNC executive later explained that the bank implemented special security measures against Plaid precisely because consumers did not understand that it "can scrape every piece of information that is in your banking relationships."[43]

100. Some Plaid employees recognized the impropriety of Plaid's efforts to circumvent banks' technical or code-based barriers to Plaid's conduct. In August 2018, a former Plaid programmer described his work on such projects in response to a prompt to describe the most unethical thing he had ever done:

[42] *See* Yuka Hayashi, *Venmo Glitch Opens Window on War Between Banks, Fintech Firms*, Wall Street Journal (Dec. 14, 2019), https://www.wsj.com/articles/venmo-glitch-opens-window-on-war-between-banks-fintech-firms-11576319402.

[43] *See* Bill Streeter, *PNC Bank Counters 'P2P War' Speculation Over Its Venmo App Moves*, The Financial Brand (Jan. 2020), https://thefinancialbrand.com/91550/pnc-bank-p2p-venmo-mobile-app-zelle-plaid-aggregator/.

> [M]any . . . banks typically forbid scraping and made it explicitly difficult by implementing JavaScript-based computational measures required on the client [side] 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 . . . and 2) performing huge amounts of analytics on customer data acquired as part of the account verification process . . . . I find it dishonest if the company mining that data is doing so without direct user consent, or in a "backdoored" manner . . . . [P]ersonally, it bothered me that so much user data would be mined from their financial statements. . . . [I]t seemed underhanded since most customers aren't aware of it. . . . But Plaid is not sold to users, it's sold to companies.[44]

VI. INJURY AND DAMAGES TO THE CLASS

101. Plaintiff and Class Members have suffered actual harm, injury, damage and loss as a result of Plaid's illegal conduct, including but not limited to economic damages and harm to their dignitary rights. Had Plaintiff and Class Members known the true nature, significance and extent of Plaid's data practices, it would not have used Plaid.

A. Plaintiff and Class Members Have Suffered Economic Damages

102. Plaid's illegal conduct caused Plaintiff and Class Members to suffer economic damages and loss, including but not limited to (a) the loss of valuable indemnification rights; (b) the loss of other rights and protections to which they were entitled as long as their sensitive personal data remained in a secure banking environment; (c) the loss of control over valuable property; and (d) the heightened risk of identity theft and fraud.

103. Plaid caused all of these damages when, without actual or constructive notice to Plaintiff and Class Members and without their knowledge or consent, Plaid (1) removed their sensitive personal data from the secure banking environment and (2) sold it to the Participating Apps and other third parties, without exercising any oversight or control over what those entities did with the data.

B. Loss of Valuable Indemnification Rights

104. Under federal regulations, a consumer is not liable for unauthorized electronic fund

[44] *See Ask HN: What Is the Most Unethical Thing You've Done As a Programmer?*, *supra* n. 29.

transfers from her financial accounts, subject to certain limits and conditions. *See, e.g.*, 12 C.F.R. § 1005.2(m). But Plaid's conduct eliminates consumers' rights to indemnification under these regulations. If Plaid's fraud and deceit induce Plaintiff and Class Members to provide their bank credentials to Plaid, and a malicious user subsequently uses those credentials to access and improperly transfer funds from Plaintiff and Class Members' accounts, banks consider that transfer to have been authorized because of the initial provision of the credentials to Plaid.[45] As noted above, JPMorgan has expressed concern that consumers do not generally understand that they will be responsible for any such loss.[46] For instance, a theft of $10,000 from a consumer's account would ordinarily leave a consumer liable for only $50; but if Plaid's conduct in any way contributes to that unlawful access, the consumer may now be liable for the full $10,000, a loss in value of $9,950. Thus, the destruction of Plaintiff and Class Members' indemnification rights is an economic loss, even if no funds are actually stolen.

C. Diminished Value of Rights to Protection of Data

105. Plaintiff and Class Members enjoy various other rights and protections relating to their sensitive personal data as long as it remains within a secure banking environment. The American Bankers Association has opined that when data aggregators like Plaid extract Plaintiff and Class Members' data from their financial institutions, it leaves the "secure bank environment, where it is accorded longstanding legal protections, and [is] released into the data services market

[45] Consumer Bankers Association Comment on Consumer Access to Financial Records (Feb. 21, 2017), *available at* https://www.consumerbankers.com/sites/default/files/CFPB%20-%20Docket%20No%20-%202016-0048%20-%20RFI%20Consumer%20Access%20to%20Financial%20Records.pdf ("If a bank customer gives their account credentials to a [planning and financial management app] PFM which subsequently initiates an unauthorized transfer or an unauthorized transfer is initiated by an outside source as a result of a breach of the PFM, the transfer would be considered authorized by the bank because the client had furnished an access device (i.e. login credentials) to the PFM, leaving the customer liable for such transfers. Accordingly, the bank would not be liable for these transfers unless the customer notified them that the transfers by the person, PFM or other vendor were no longer authorized."); *see also* Response by American Bankers Association to CFPB RFI (Feb. 21, 2017), 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.

[46] *Letter from JPMorgan Chase to Shareholders*, *supra* n. 41.

where it is accorded no more special status than data created through a consumer's use of a social media platform."[47] By removing Plaintiff and Class Members' data from the secure bank environment and storing it in its own computer systems, networks or servers, Plaid has destroyed the rights and protections to which Plaintiff and Class Members are otherwise entitled. That amounts to an economic loss to Plaintiff Class Members.

D. Loss of Control Over Valuable Property

106. The data that Plaid collects, retains and sells has enormous value both to Plaid itself and to the Plaintiff and Class Members from whom Plaid illicitly obtains it. First of all, the data at issue is clearly of value to Plaid. In January 2020, Visa announced an acquisition of Plaid for $5.3 billion, based in no small part on the universe of consumers that Plaid has accumulated. Further, Plaid has pivoted its business from aggregating that data to analyzing and packaging it for the Participating Apps and other third party customers, thus demonstrating that there is an active market for Plaintiff and Class Members' data. The sheer size of this mountain of data, as well as Plaid's ability to continue accessing Plaintiff and Class Members' transaction histories on an ongoing basis—as many as 4-6 times a day—creates a competitive advantage that Plaid may exercise over its competitors. All of these facts indicate that the data Plaid gathers is valuable. Once Plaid acquires it, however, Plaintiff and Class Members have no control over what Plaid does with it, including how it packages it and to whom it sells it. Further, Plaid exercises no oversight or control over this data after it sells it. Thus, Plaintiff and Class Members suffered economic loss from the loss of control over their valuable property.

E. Increased Risk of Identity Theft and Fraud

107. Plaid's conduct not only destroyed Plaintiff and Class Members' rights to indemnification in the event their accounts are compromised, but has also increased the risk of just such an incident occurring. As the ABA has recognized, the "sheer volume and value of the aggregated data" warehoused at entities like Plaid makes them "a priority target for criminals, including identity thieves." Databases like Plaid's create a one-stop shop for such malicious actors

[47] American Bankers Association Comment on Consumer Access to Financial Records, *supra* n. 45.

to gain access to all of a consumer's accounts, creating a "rich reward for a single hack." Plaid's consolidation of risk to consumers at a single point of entry creates tangible, economic injury to Plaintiff and Class Members, who now must spend time and money closely monitoring their credit report and other financial records for any evidence that their accounts have been compromised. Plaid's conduct has permanently impaired the integrity of Plaintiff and Class Members' bank accounts and the banking information and data therein. Plaintiff and Class Members now face an expanded and imminent risk of economic harm from unauthorized transfers, identity theft, and fraud.

F. Plaintiff and Class Members Have a Reasonable Expectation of Privacy in the Data that Plaid Gathers

108. When Plaid obtains the login credentials for a user, it gains access to a vast trove of that user's sensitive personal data, including transaction history going back as much as five years. Even if a user only connects a single account to one of the Participating Apps, Plaid gains access to *all* accounts that a user associates with those login credentials, including checking, savings, and retirement or other investment accounts, as well credit card and loan accounts. Plaid thus accesses data about the most intimate facts of Plaintiff and Class Members' lives, including without limitation information about their income, charitable giving, retirement contributions, healthcare costs and treatment, shopping habits, dining habits, entertainment habits, saving and spending habits, credit repayment habits, and loan terms, as well as other financial affairs. Plaid implements no precautions to ensure that it does *not* capture data that may be protected by HIPAA, including information regarding medical procedures, doctor's visits or prescriptions. Plaid also collects personal identifying information such as a user's name, address, email address and phone number, as well as employment information such as the identity of a user's employer and her salary. Plaid takes no steps to avoid collecting data about minors, whose accounts Plaid may well have accessed and about whom Plaid would have collected data as long as a Class member was a custodian for a relevant account. The data Plaid accesses, collects, and retains is not only broad—by Plaid's own estimate, it includes thousands of transactions for every individual—but also deep, including such details as the amount paid, to whom, and the date and geographic location of the transaction.

109. Plaintiff and Class Members have a reasonable expectation of privacy in this data. Various statutes, Constitutional provisions and centuries of common law support this presumption as to users' sensitive personal data in general, and as to their financial data or health data in particular.

110. A series of surveys by The Clearing House ("TCH"), a banking association and payments company, confirmed how important it is to most consumers that such data remain private, as well as the general lack of understanding among consumers of how invasive the data practices of aggregators like Plaid can be. One such survey concluded that the vast majority of consumers are unaware of what data companies like Plaid collect or for how long it is accessed. As many as 89% of consumers are concerned, very concerned or extremely concerned about data privacy with regard to Fintech apps.

111. Plaintiff and Class Members had a reasonable expectation of privacy in the sensitive personal information discussed herein. Plaid's collection, retention and sale of that information invaded Plaintiff and Class Members' privacy and harmed their dignitary rights.

G. Plaid Violates Users' Reasonable Expectations of Privacy in Highly Offensive Ways that Amount to Egregious Violations of Social Norms

112. Plaid's collection, retention and sale of Plaintiff and Class Members' sensitive personal data would be highly offensive to the reasonable person. Plaid's conduct goes far beyond what would be considered routine commercial behavior, even among other fintech apps. It violates various social norms as identified in legislative and constitutional provisions, as well as various expressions of public policy and the common law, for at least the following reasons:

1. Plaid's collection, storage and use of data is far out of proportion to what Plaid needs to link users' accounts to Participating Apps, including because Plaid collects massive troves of data going back five years and going forward in perpetuity;

2. Plaid deceives users into thinking that they are entering their credentials directly with their trusted financial institutions, when in fact they are providing those credentials to Plaid for Plaid's permanent retention and use;

3. Plaid retains the data that it collects indefinitely;

4. Plaid profits from the data it collects in ways that it fails to disclose to Plaintiff and Class Members;

5. The nature of the data that Plaid collects reaches into every part of users' lives; and

6. Users did not consent to Plaid's invasion of their privacy because Plaid failed to disclose the scope and nature of its data practices, thus rendering any consent it obtained from users ineffective or, at the least, narrower than the conduct in which Plaid engages.

H. Other Damages

113. Plaid's conduct damaged Plaintiff and Class Members in other ways, including because Plaid:

1. impaired the integrity of the Plaintiff and Class Members' data by storing it on its own systems and using it for its own purposes;

2. impaired the integrity of the financial institutions' protected computers by increasing the number of entities that have access to such data;

3. failed to monitor or oversee third party customers to whom Plaid sold Plaintiff and Class Members' data and/or analytics products based on this data;

4. impaired the integrity of Plaintiff and Class Members' smartphones by installing software within the Participating Apps that captured their bank login credentials; and

5. caused Plaintiff and Class Members mental and emotional distress.

VII. CHOICE OF LAW

114. California's substantive laws may be constitutionally applied to the claims of Plaintiff 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.

115. California has a significant contact, or significant aggregation of contacts, to the claims asserted by Plaintiff and the Class, 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 in, was implemented in and emanated from California. Plaid collects and stores Plaintiff and Class

Members' data in California, and sells it from California. California has a stronger interest in regulating Plaid's conduct under its laws than any other state.

116. The application of California law to the proposed Nationwide Class 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

117. The statutes of limitation applicable to Plaintiff's claims are tolled as a result of Plaid's knowing and active concealment of its conduct alleged herein. Among other things, Plaid and its co-founders made a series of misrepresentations and omissions in the software it embeds in the Participating Apps; in its Privacy Policy; and in its public statements, including in interviews, in postings on online forums, and in submissions to government agencies and regulators. Plaid intentionally concealed the nature and extent of its actions and intentions. To the extent the Participating Apps made statements regarding Plaid's service or its privacy policies, Plaid either approved those statements or failed to timely correct them in service of its ongoing scheme to conceal the true nature of its conduct.

118. Plaintiff and Class Members could not, with due diligence, have discovered the full scope of Plaid's conduct, due in no small part to Plaid's deliberate efforts to conceal it. All applicable statutes of limitation also have been tolled by operation of the discovery rule. Under the circumstances, Plaid was under a duty to disclose the nature and significance of its data and privacy policies and practices, but did not do so. Plaid therefore is estopped from relying on any statute of limitations.

119. Plaid's fraudulent concealment and omissions are common to Plaintiff and all Class Members.

IX. CLASS ACTION ALLEGATIONS

120. Plaintiff incorporates by reference all the foregoing allegations. Plaintiff brings this action on behalf of herself and all others similarly situated pursuant to Rule 23(b)(2) and 23(b)(3) of the Federal Rules of Civil Procedure.

121. Plaintiff seeks to represent the following Classes:

> **Nationwide Class:** All natural persons in the United States whose accounts at a financial institution Plaid accessed by using login credentials that Plaid obtained through software incorporated in a mobile or web-based software application 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 Plaid accessed by using login credentials that Plaid obtained through software incorporated in a mobile or web-based software application 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.

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

123. 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).

124. **Numerosity**. Plaintiff possesses no knowledge or information regarding the exact size of the Classes or the identities of the Class Members. On information and belief, and based on Plaid's own statements that as many as 1 in 4 natural persons in the United States have used Plaid and that Plaid has accessed as many as 200 million financial accounts, each Class has thousands or millions of members. Thus, the number of members in each Class is so numerous that joinder is impracticable. Plaid possesses information sufficient to identify the Class Members.

125. **Commonality**. Common questions of law and fact exist as to all members of the Classes. This is particularly true given the nature of Plaid's conduct, which was generally applicable to all the members of both Classes, calling for relief for the Classes as a whole. Such questions of law and fact common to the Classes include, but are not limited to:

1. Whether a reasonable person would have a reasonable expectation of privacy in the information that Plaid collected from them;

2. Whether Plaid's conduct was highly offensive to a reasonable person and/or amounted to an egregious breach of social norms;

3. Whether Plaid violated the federal Stored Communications Act and Computer Fraud and Abuse Act;

4. Whether Plaid violated California's Comprehensive Data Access and Fraud Act, Unfair Competition Law, Anti-Phishing Act, and Civil Code §1709;

5. Whether Plaid unjustly enriched itself to the detriment of Plaintiff and Class Members, thereby entitling Plaintiff and Class Members to disgorgement of all benefits derived by Defendants;

6. Whether Plaid acted negligently;

7. Whether the conduct of Plaid and its co-conspirators, as alleged in this Complaint, caused harm, injury, damage or loss to Plaintiff and Class Members;

8. The appropriate injunctive and equitable relief; and

9. The appropriate class-wide measure of damages.

126. **Predominance**. The questions of law and fact common to the members of the Classes predominate over any questions affecting only individual members, including legal and factual issues relating to liability and damages. The most important questions at issue involve Plaid's conduct, which was common to all or nearly all members of the Classes. Questions relating to the applicability of statutory and common law as well as the scope or presence of injuries are also common to the Classes.

127. **Typicality**. Plaintiff's claims are typical of those of all or nearly all members of the Classes because Plaid's conduct applied to all or nearly all members of the Classes in identical or nearly identical ways. Plaintiff's claims and those of Class Members arise from the same operative facts and legal theories. Plaid cannot articulate any defenses that are unique to Plaintiff.

128. **Adequacy**. Plaintiff is an adequate representatives of the Classes. Plaintiff's claims arise out of the same common course of conduct giving rise to the claims of the other members of the Classes. Plaintiff's interests are coincident with, and not antagonistic to, those of the other members of the Classes. Plaintiff is represented by counsel who are competent and experienced in the prosecution of antitrust and class action litigation. Plaintiff intends to prosecute this action vigorously. Plaintiff and her counsel will fairly and adequately protect the interest of the Classes.

129. **Superiority**. Class action treatment is a superior method for the fair and efficient

adjudication of the controversy, in that, among other things, such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort and expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities with a method for obtaining redress for claims that might not be practicable to pursue individually, substantially outweigh any difficulties that may arise in the management of this class action. Classwide adjudication benefits Plaintiff, Defendant, and the court system by addressing similar or identical claims related to Plaid's illicit conduct universally and at once, while avoiding the potential for inconsistent or contradictory judgments.

130. **Injunctive Class**. Class certification under Rule 23(b)(2) for purposes of injunctive and declaratory relief is warranted because Plaid acted or refused to act—and continues to act or refuse to act—in ways that apply generally to the Classes, such that final injunctive and declaratory relief are appropriate with respect to, and would benefit, the Classes as a whole.

X. CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION

Common Law Invasion of Privacy—Intrusion Upon Seclusion

131. Plaintiff incorporates the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

132. Plaintiff brings this claim on behalf of herself and the Nationwide Class or, in the alternative, the California Class, under California law.

133. Plaid intruded upon Plaintiff and Class Members' seclusion by collecting, retaining and selling data (1) in which they had a reasonable expectation of privacy for the reasons described herein; and (2) in a manner that was highly offensive to Plaintiff and Class Members, would be highly offensive to a reasonable person, and was in egregious violation of social norms for the reasons described herein.

134. Plaid's conduct described herein violations Plaintiff and Class Members' interests in avoiding the dissemination of sensitive personal data about their financial and other affairs (i.e.,

their informational privacy rights), as well as their interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference (*i.e.*, their autonomy privacy rights).

135. Plaintiff and Class Members suffered actual harm, injury, damage and loss as a result of Plaid's conduct as alleged herein.

136. Plaintiff and Class Members are entitled to appropriate relief, including compensatory damages for the harm to their privacy and dignitary interests, loss of valuable rights and protections, heightened risk of future invasions of privacy, and mental and emotional distress. Plaintiff and Class Members are entitled to an order requiring Plaid to disgorge profits or other benefits that Plaid acquired as a result of its invasions of privacy. Plaintiff and Class Members are entitled to punitive damages resulting from the malicious, willful and intentional nature of Plaid's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Plaid from engaging in such conduct in the future. Plaintiff also seeks such other relief as the Court may deem just and proper.

SECOND CAUSE OF ACTION

Violation of Article I, § 1 of the California Constitution

137. Plaintiff incorporates the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

138. Plaintiff brings this claim on behalf of herself and the California Class.

139. The California Constitution provides that all people by nature have certain inalienable rights, including "pursuing and obtaining safety, happiness, and privacy." Cal. Const., art. I, § 1.

140. Plaid violated Plaintiff and California Class Members' Constitutional right to privacy by collecting, retaining and selling data (1) in which they had a reasonable expectation of privacy for the reasons described herein; and (2) in a manner that was highly offensive to Plaintiff and Class Members, would be highly offensive to a reasonable person, and was in egregious violation of social norms for the reasons described herein.

141. Plaintiff and California Class Members suffered actual and concrete injury as a

result of Plaid's violations of their Constitutional rights and are entitled to all appropriate relief, as alleged herein.

THIRD CAUSE OF ACTION

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

142. Plaintiff incorporates the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

143. Plaintiff brings this claim on behalf of herself and the Nationwide Class.

144. The SCA prohibits a person from (1) intentionally accessing without authorization, or in excess of authorization, a facility through which an electronic communication service ("ECS") is provided and (2) thereby obtained, altered, or prevented authorized access to a wire or electronic communication (3) while it was in electronic storage in such system. 18 U.S.C. § 2701(a)(1).

145. The data that Plaid collects from the financial institutions are electronic communications. The SCA defines "electronic communication" broadly to include "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. 2510(12).[48] The data that Plaid illicitly acquired from Plaintiff and Class Members' financial accounts are electronic communications within the statute.

146. The bank servers and systems that Plaid accesses are facilities that provided ECS, within the definition of the statute. An ECS provider is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). The financial institutions to which Plaid connects provide various economic communications services to their customers as part of their commercial offerings, including by sending, receiving, posting and making available for transfer messages, data, images, queries, notifications, statements, forms, updates, and others. *See* 18 U.S.C. § 2510(15) (defining "electronic communication service").

147. The electronic communications that Plaid accesses from financial institution servers

[48] Notably, the definition "does not include . . . (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds." *Id.* Thus, this cause of action does not apply to such electronic funds transfer information, although other causes of action herein may apply to such information.

and systems are kept in electronic storage by those institutions. The SCA defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17). The financial institutions with which Plaid interacts maintain the electronic communications that Plaid collects both for temporary or intermediate storage as well as for purposes of backup protection. They are maintained in systems, servers and databases both for record-keeping as well as for access by consumers.

148. Plaid intentionally accessed these facilities without authorization from Plaintiff and Class Members. Any authorization that Plaintiff and Class Members may purportedly have provided to Plaid is null, void, invalid and ineffective because: Plaid obtained any such authorization by fraud and deceit; Plaid failed to provided Plaintiff and Class Members with actual or constructive notice of the nature and significance of Plaid's data and privacy practices; Plaid's Privacy Policy contains material misrepresentations and omissions; Plaintiff and Class Members never voluntarily downloaded or installed any application that Plaid offered; and Plaintiff and Class Members were not on notice that Plaid was an entity distinct from the Participating App(s) they signed up to use. To the extent Plaid obtained any valid authorization at all, Plaid nonetheless accessed these facilities far in excess of the authorization it received by obtaining data beyond what was needed to validate users' bank accounts, storing it for longer than necessary, continuing to collect data as often as once every 4-6 hours even months or years after users first tried to connect a bank account, and selling that data to undisclosed third parties.

149. Plaintiff and Class Members suffered concrete and particularized injury resulting from Plaid's violations of the SCA as alleged herein. Plaintiff and the Class are entitled to damages, equitable or declaratory relief, and reasonable attorney's fees, pursuant to 18 U.S.C. § 2707. Plaintiff also seeks such other relief as the Court may deem just and proper.

150. Plaintiff 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. Thus, this action is timely under 18 U.S.C. § 2707(f).

FOURTH CAUSE OF ACTION

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

151. Plaintiff incorporates the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

152. Plaintiff brings this claim on behalf of herself and the Nationwide Class.

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

153. A person violates 18 U.S.C. § 1030(a)(2) if it "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—(A) information contained in a financial record of a financial institution . . . [or] (C) information from any protected computer." Protected computers include computers "exclusively for the use of a financial institution . . . or . . . used by . . . a financial institution . . . and the conduct constituting the offense affects that use by or for the financial institution," 18 U.S.C. § 1030(e)(2)(A), or computers "used in or affecting interstate or foreign commerce," 18 U.S.C. § 1030(e)(2)(B).

154. The computer systems, data storage facilities, or communications facilities that Plaintiff and Class Members' financial institutions use to store Plaintiff and Class Members' data are "protected computers" under the statute because they are exclusively for the use of financial institutions or, in the alternative, were affected by Plaid's conduct, or were used in or affected interstate commerce. Plaid intentionally accessed these protected computers and thereby obtained information contained in the financial institutions' financial records. Plaid did so without authorization because the consent that Plaid purported to receive from Plaintiff and Class Members was null, void, invalid and ineffective for the reasons described above. To the extent Plaid received any valid authorization, its conduct exceeded that authorization for the reasons described above. *See* 18 U.S.C. 1030(e)(6) (defining the term "exceeds authorized access" to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter").

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

155. A person violates 18 U.S.C. § 1030(a)(4) if it "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means

of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period."

156. Plaid knowingly accessed protected computers, and did so without authorization or in excess of authorization, for the reasons described herein.

157. Plaid acted with intent to defraud because it devised an elaborate scheme to deceive Plaintiff and Class Members into thinking that they were providing their banking credentials directly to their bank, when in fact they were providing those credentials to Plaid. Through that conduct, Plaid furthered its fraud and obtained things of value, namely, Plaintiff and Class Members' sensitive personal data.

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

158. A person violates 18 U.S.C. § 1030(a)(5)(A) if it "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer."

159. Plaid knowingly caused the transmission of a program, information, code or command every time it sent Plaintiff and Class Members' credentials to their financial institutions. Plaid did so without authorization for the reasons described herein. Plaid caused damage for the reasons described herein.

4. **Violations of 18 U.S.C. § 1030(a)(5)(B), (C)**

160. A person violates 18 U.S.C. § 1030(a)(5)(B) if it "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage." A person violates 18 U.S.C. § 1030(a)(5)(C) if it "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss."

161. Plaintiff and Class Members' financial institutions' computer systems, data storage facilities, or communications facilities are protected computers under the statute for the reasons described herein. Plaid acted without authorization for all of the reasons described herein. Plaid acted not only recklessly but intentionally for all of the reasons herein. Plaid caused damage or loss for the reasons described herein.

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

162. A person violates 18 U.S.C. 1030(a)(6) if it "knowingly and with intent to defraud traffics . . . in any password or similar information through which a computer may be accessed without authorization, if—(A) such trafficking affects interstate or foreign commerce." The term "traffic" means "transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of." 18 U.S.C. 1029 (e)(5).

163. Plaid acted knowingly and with intent to defraud for the reasons described herein. Plaid acted without authorization for the reasons described herein. Plaid trafficked in passwords and similar information when it obtained control of banking credentials from as many as 200 million distinct financial accounts with the intent of transferring them to its own massive database of user information, thus allowing Plaid access to Plaintiff and Class Members' financial institutions' computers. In the alternative, Plaintiff trafficked in passwords and similar information when, after acquiring Plaintiff and Class Members' login credentials under false pretenses and using them to login to those individuals' financial institutions, those institutions sent access tokens to Plaid, which access tokens Plaid then transferred to the Participating Apps.

164. On information and belief, because of the locations of Plaid, its servers, the 200 million accounts for which Plaid acquired credentials and data, and the 11,000 financial institutions to which Plaid has access, Plaid's trafficking activities affected interstate or foreign commerce.

6. **Plaid Caused Economic Loss in Excess of $5,000, as Well as other Damage**

165. Plaintiff may bring a private right of action for economic damages resulting from Plaid's violation of the CFAA, provided that they caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." 18 U.S.C. 1030 (c)(4)(A)(i)(I). The CFAA defines the term "damage" to include "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). The CFAA defines the term "loss" to include "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages

incurred because of interruption of service." 18 U.S.C. 1030(e)(11).

166. Each of the violations detailed above caused economic loss to Plaintiff and Class Members that exceeds $5,000 per year individually or in the aggregate. In particular, Plaid caused losses to Plaintiff and Class Members by imposing unreasonable costs on them, including the cost of conducting damage assessments, restoring the data to its condition prior to the offense, and consequential damages they incurred by, inter alia, spending time conducting research to ensure that their identity had not been compromised and accounts reflect the proper balances.

167. Plaid's violations damaged Plaintiff and Class Members in other ways as described herein. Plaintiff seeks such other relief as the Court may deem just and proper.

168. Plaintiff brings this cause of action within two years of the date of the discovery of their damages. Thus, this action is timely under 18 U.S.C. § 1030(g).

FIFTH CAUSE OF ACTION

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

169. Plaintiff incorporates the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

170. Plaintiff brings this claims on behalf of herself and the Nationwide Class or, in the alternative, the California Class, under California law.

171. A person violates the CDAFA if it commits one of 14 acts.

172. A person violates Cal. Penal Code §502(c)(1) if it "*[k]nowingly accesses* and *without permission alters, damages, destroys, or otherwise uses . . . any data*, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive or extort, or (B) wrongfully control or obtain money, property or data." (Emphasis added.) Plaid violated §502(c)(1) when it accessed Plaintiff and Class Members' sensitive personal information and damaged and used Plaintiff and Class Members' sensitive personal information. Plaid acted without permission for the reasons described herein. Plaintiff and Class Members had no notice, whether actual or constructive, that Plaid was a separate entity from the Participating Apps, and thus no notice that Plaid was operating; had no way to remove Plaid's software; and do

not have an opportunity to consent to Plaid's access to their sensitive personal data each time that Plaid accesses it, which can be as often as 4-6 times per day. Plaid accessed and used this data in order to execute its scheme to defraud and deceive, because Plaid employed fraud and deceit to induce Plaintiff and Class Members to turn over their financial institution login credentials to Plaid. Additionally, Plaid accessed and used this data to wrongfully obtain money, property or data, both because it obtained the data under false pretenses and because it used the data to develop analytics products that it then sold to Participating Apps and other customers.

173. A person violates Cal. Penal Code §502(c)(2) if it "*[k]nowingly accesses* and *without permission* takes, copies, or *makes use of any data* from a computer, computer system, or computer network." (Emphasis added.) Plaid violated §502(c)(2) when it accessed Plaintiff and Class Members' sensitive personal information without permission as described herein, and made use of Plaintiff and Class Members' sensitive personal information without permission as described herein.

174. A person violates Cal. Penal Code §502(c)(3) if it "*[k]nowingly and without permission uses or causes to be used computer services.*" (Emphasis added.) Plaid violated §502(c)(3) when it knowingly and without permission used or caused to be used the computer services of Plaintiff and Class Members' financial institutions, as described herein.

175. A person violates Cal. Penal Code §502(c)(4) if it "*[k]nowingly accesses and without permission* adds, alters, *damages*, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network." (Emphasis added.) Plaid violated §502(c)(4) when it knowingly damaged Plaintiff and Class Members' sensitive personal data, and damaged Plaintiff and Class Members' financial institutions' computers, computers systems and computer networks, as described herein. Plaid acted without permission for the reasons described herein.

176. A person violates Cal. Penal Code §502(c)(6) if it "*[k]nowingly and without permission provides or assists in providing a means of accessing* a computer, computer system, or computer network in violation of this section." (Emphasis added.) Plaid violated §502(c)(6) when it knowingly used Plaintiff and Class Members' login credentials, which it obtained under false

pretenses, and provided them to Plaintiff and Class Members' financial institutions, as described herein. Plaid acted without permission for the reasons described herein.

177. A person violates Cal. Penal Code §502(c)(7) if it "*[k]nowingly and without permission accesses or causes to be accessed* any computer, computer system, or computer network." (Emphasis added.) Plaid violated §502(c)(7) when it knowingly used Plaintiff and Class Members' login credentials, which it obtained under false pretenses, to access the computers, computer systems and computer networks of Plaintiff and Class Members' financial institutions, as described herein. Plaid acted without permission for the reasons described herein.

178. Plaid accessed the data, computers, computer systems and computer networks above in ways that circumvented technical or code-based barriers.

179. Plaintiff and Class Members are owners of the sensitive personal data that Plaid collected, retained and sold, and suffered actual harm, injury, damage and loss as a result of Plaid's conduct, as described herein. Thus, Plaintiff and Class Members may bring a civil action for compensatory damages, including "expenditure[s] reasonably and necessarily incurred . . . to verify that . . . data was or was not altered, damaged or deleted by access." Cal. Pen. Code §502(e)(1). Further, Plaid shall pay punitive and/or exemplary damages because its violations were willful. *Id.* § 502(e)(4). Plaintiff shall be entitled to reasonable attorney's fees. *Id.* § 502(e)(2). Plaintiff also seeks such other relief as the Court may deem just and proper.

SIXTH CAUSE OF ACTION

Unjust Enrichment

180. Plaintiff incorporates the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

181. Plaintiff brings this claim on behalf of herself and the Nationwide Class (referred to in this claim as "the Class") under California law, or in the alternative, the law of the fifty states.

182. Plaid received benefits from Plaintiff and Class Members and unjustly retained those benefits at their expense.

183. In particular, Plaid received benefits from Plaintiff and Class Members in the form of the sensitive personal data that Plaid collected from Plaintiff and Class Members, without

authorization and as a product of the deceitful conduct described herein. Plaid has compiled that data into an "immense" database, which it has packaged into various products that have provided Plaid with economic, intangible, and other benefits.

184. Plaid unjustly retained those benefits at the expense of Plaintiff and Class Members because Plaid's conduct damaged Plaintiff and Class Members as described herein, all without providing any commensurate compensation to Plaintiff and the Class.

185. The benefits that Plaid derived from Plaintiff and Class Members rightly belong to Plaintiff and Class Members. It would be inequitable under unjust enrichment principles in California and every other state for Plaid to be permitted to retain any of the profit or other benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

186. Plaid should be compelled to disgorge in a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds it received, and such other relief as the Court may deem just and proper.

SEVENTH CAUSE OF ACTION

Violation of California's Anti-Phishing Act of 2005, Cal. Bus. & Prof. Code § 22948.2

187. Plaintiff incorporates the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

188. Plaintiff brings this claim on behalf of herself and the Nationwide Class or, in the alternative, the California Class.

189. The California Anti-Phishing Act of 2005 (the "Anti-Phishing Act") makes it unlawful to use 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." Cal. Bus. & Prof. Code § 22948.2. "Identifying information" includes bank account numbers, account passwords, and "[a]ny other piece of information that can be used to access an individual's financial accounts." Cal. Bus. & Prof. Code § 22948.1(b). An individual who is adversely affected by a violation of Section 22948.2 may bring an action. Cal. Bus. & Prof. Code §22948.3(a)(2).

190. As described herein, Plaid violated the Anti-Phishing Act by representing itself to be Plaintiff and Class Members' financial institutions. Plaid fraudulently and deceitfully impersonated those institutions in order to induce Plaintiff and Class Members to provide their login credentials to Plaid, as described herein. Plaid did so without obtaining the authority or approval of each financial institution.

191. Plaintiff and Class Members have been adversely affected by Plaid's violations of the Anti-Phishing Act because Plaid engaged in this deceitful conduct in order to extract from Plaintiff and Class Members their login credentials and all of the transaction history and other data accessible with those credentials, as detailed above. Plaid caused actual injury harm, damage and loss to Plaintiff and Class Members for the reasons described herein.

192. Plaintiff and Class Members are entitled to relief under Cal. Bus. & Prof. Code § 22948.3(a)(2), including $5,000 per violation, which damages should be trebled because Plaid engaged in a pattern and practice of violating § 22948.2 (indeed, it is the essence of Plaid's business model); an injunction against further violations; costs of suit and reasonable attorney's fees; and such other relief as the Court may deem just and proper.

EIGHTH CAUSE OF ACTION

Violation of California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200

193. Plaintiff incorporates the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

194. Plaintiff brings this claims on behalf of herself and the Nationwide Class or, in the alternative, the California Class.

195. Plaid's conduct as alleged herein constitutes unlawful, unfair, and/or fraudulent business acts or practices as prohibited by the UCL.

1. **"Unlawful"**

196. Plaid's conduct constitutes an unlawful business practice within the meaning of the UCL because it violates, without limitation, the following: the CFAA, the SCA, the CDAFA, the GLBA's Privacy Rule, CalFIPA, Cal. Pen. Code § 502, California's Anti-Phishing Act of 2005, the CCPA, CalOPPA, Cal. Civ. Code § 1709 and Article 1, § 1 of the California Constitution.

2. **"Unfair"**

197. Plaid's conduct separately constitutes an unfair business practice within the meaning of the UCL because Plaid's practices have caused and are likely to cause substantial injury to the Plaintiff and the members of the Class that is not reasonably avoidable by them.

198. Plaid's conduct, as alleged herein, is and was contrary to public policy, immoral, unethical, oppressive, unscrupulous and/or substantially injurious to consumers. Among other things, it is contrary to the public policy in favor of protecting consumer data in general and consumer financial data in particular. Any purported benefits arising out of Plaid's conduct do not outweigh the harms caused to the victims of Plaid's conduct.

199. Plaid's conduct is also unfair because it is contrary to numerous legislatively declared policies, as set forth in the CFAA, the SCA, the CDAFA, the GLBA's Privacy Rule, CalFIPA, Cal. Pen. Code § 502, California's Anti-Phishing Act of 2005, the CCPA, CalOPPA, Cal. Civ. Code § 1709 and Article 1, § 1 of the California Constitution, which explicitly recognizes every individual's right to privacy. Here, Plaid's conduct not only violates the letter of the law, but also contravenes the spirit and purpose of each of those laws.

200. Plaid's conduct is unfair because the harm to the victim outweighs any benefits. Plaid's deceitful and illicit collection of Plaintiff and Class Members' sensitive personal data are against public policy in a myriad of ways, including the statutes above that explicitly protect individuals' privacy interests in their personal data in general and the data they store with their financial institutions in particular. The conduct alleged herein threatens an incipient violation of each of those laws and has both an actual and a threatened impact on competition.

201. Plaid's conduct is unfair because Plaid's Privacy Policy contained material misrepresentations and omitted material facts that were necessary to make the policy not false and misleading, as described herein.

202. Plaid's conduct is unfair because the data it collected and the time for which it stored that data violate the principle of data minimization to which Plaid itself claims to subscribe, in particular because Plaid's collection, storage and sale of Plaintiff and Class Members' data is wholly disproportionate to that needed to provide the service Plaid ostensibly provided to Plaintiff

and Class Members—namely, connecting their bank accounts to a Participating App.

3. **"Fraudulent"**

203. Plaid's conduct, as described herein, constitutes a fraudulent business practice within the meaning of the UCL. Plaid has only been able to amass the mountain of data on which its business is based by deceiving Plaintiff and Class Members that they were using their login credentials to access their financial institutions directly, when in fact they were providing those credentials to Plaid for its own purposes. Plaid deceived Plaintiff and Class Members into thinking that the bank login protocol was "secure" and "private," when it was not. Plaid designed its interface to deceive—and did deceive—Plaintiff and Class Members in order to fraudulently obtain access to their detailed financial histories going back as much as five years and going forward in perpetuity.

204. Members of the public would likely have been deceived by Plaid's actions. Plaintiff and Class Members relied on and were harmed by those actions.

4. **Injury**

205. Plaintiff and Class Members have suffered injury in fact and lost money or property as a result of Plaid's conduct as described herein.

206. Plaintiff and Class Members are entitled to equitable and injunctive relief including restitution and restitutionary disgorgement. Plaintiff is also entitled to an injunction prohibiting Plaid from collecting, storing and/or selling Plaintiff and Class Members' sensitive personal data on a going forward basis, and requiring Plaid to destroy any login credentials that it obtained as a result of the conduct described herein. Plaintiff also seeks such other relief as the Court may deem just and proper.

NINTH CAUSE OF ACTION

Violation of Cal. Civ. Code § 1709

207. Plaintiff incorporates the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

208. Plaintiff brings this claim on behalf of herself and the Nationwide Class or, in the alternative, the California Class.

209. California Civil Code § 1709 provides that "[o]ne who willfully deceives another with intent to induce him to alter his position to his injury or risk, is liable for any damage which he thereby suffers." A defendant violates §1709 if (i) it had a duty to disclose a material fact to the plaintiff; (ii) it intentionally concealed that fact with intent to defraud; (iii) plaintiff was unaware of that fact (and would have acted differently if he were aware), and (iv) plaintiff sustained some damage as a result. California Civil Code § 1710 defines "deceit" as "1. [t]he suggestion, as a fact, of that which is not true, by one who does not believe it to be true; 2. [t]he assertion, as a fact, of that which is not true, by one who has no reasonable ground for believing it to be true; 3. [t]he 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."

210. Plaid engaged in various acts of deceit. Plaid either suggested that certain facts are true which it knew were not true, or which it had no reasonable ground for believing to be true. Examples of such statements include but are not limited to statements (that Plaid either made itself or of which Plaid was aware) that Plaintiff and Class Members' transmission of login credentials to their financial institutions were "secure" and "private," when in fact Plaid was intercepting them; and that Plaid always acts in consumers' best interests, when in fact it impairs the integrity of Plaintiff and Class Members' sensitive personal data to their detriment and for Plaid's benefit. Plaid suppresses facts and provides other facts that are likely to mislead, as described herein. Plaid also led Plaintiff and Class Members to believe that they were providing their credentials directly to their banks, when in fact Plaid knew that fact was not true because Plaintiff and Class Members were providing their credentials directly to Plaid.

211. Plaid willfully engaged in these acts of deceit with intent to induce Plaintiff and Class Members to alter their position to their injury or risk, namely by turning over their bank credentials to Plaid under false pretenses. Plaid had a duty to disclose these facts to Plaintiff and Class Members; it intentionally concealed those facts with intent to defraud; Plaintiff and Class Members were unaware of these facts, and would have acted differently if they were aware; and Plaintiff and Class Members sustained damage as a result.

212. Plaintiff and Class Members seek recovery of their resulting damages, including economic damages, restitution, and disgorgement, as well as punitive damages and such other relief as the Court may deem just and proper.

TENTH CAUSE OF ACTION

Negligence

213. Plaintiff incorporates the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

214. Plaintiff brings this claim on behalf of herself and the Nationwide Class (referred to in this claim as "the Class") under California law, or in the alternative, the law of the fifty states.

215. Plaid owed legal duties to Plaintiff and Class Members, including the duty to timely disclose the full scope and extent of its data practices. Timely disclosure was necessary to enable Plaintiff and Class Members to, among other things, monitor their online presence to ensure it has not been coopted for illicit purposes; undertake appropriate measures to avoid unauthorized charges on their financial accounts; purchase credit monitoring services; change or cancel any credentials they maintained with online or mobile accounts for their financial accounts; and/or delete the accounts they maintained with Participating Apps. Plaid also had duties to minimize its data collections; to take reasonable security measures to protect Plaintiff and Class Members' data, including by encrypting any transfer of such data; and to exercise control and oversight over third parties to whom it sold that data.

216. Plaid has acknowledged these duties as described herein.

217. Plaid breached its duties by failing to disclose to Plaintiff and Class Members the full extent of or sufficient detail regarding its data practices; by collecting and retaining far more data than was necessary for the services that it provided to Plaintiff and Class Members; by continuing to collect such data after Plaid provided any service to Plaintiff and Class Members; for failing to encrypt or otherwise prevent unauthorized access to that data; by removing such data from the secure banking environment; by failing to require sufficient disclosures in the Plaid Link software that it embeds in the Participating Apps; and by failing to exercise any oversight over third parties to whom Plaid sold Plaintiff and Class Members' data, including when packaged into the

analytics products as described herein.

218. Plaid's violation of its duties caused Plaintiff and the other Class Members' actual harm and damages, as described herein.

219. It was foreseeable that Plaid's conduct would injure Plaintiff and Class Members. Indeed, such injuries were more than foreseeable; they are the heart of Plaid's business model.

220. At all relevant times, Plaintiff and Class Members acted lawfully and with due care and did not contribute to the injuries suffered.

221. Plaintiff and Class Members seek recovery of their resulting damages, including economic damages, restitution, and disgorgement. Plaid's negligence constituted a willful and conscious disregard of the rights of Plaintiff and the Class members, such that an award of punitive damages is appropriate. Plaintiff also seeks such other relief as the Court deems just and proper.

XI. PRAYER FOR RELIEF

222. Plaintiff requests that judgment be entered against Plaid and that the Court grant the following:

1. An order determining that this action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiff is Class Representative, and that Class notice be promptly issued;
2. Judgment against Plaid for Plaintiff and Class Members' asserted claims for relief;
3. Appropriate declaratory relief against Plaid;
4. Equitable and injunctive relief requiring Plaid to:
    a) purge the data it has unlawfully collected, including Plaintiff's and all Class Members' login credentials and transaction data;
    b) cease using any login credentials to access any financial institution;
    c) implement a permission protocol that complies with the industry-standard of OAuth 2.0, including by providing that Plaid shall not obtain or retain any user credentials;
    d) plainly and conspicuously disclose, on the first screen of the Plaid Link software, as it appears in any Participating App:
        1) 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;
        2) that Plaid will not collect or retain any data beyond what is necessary to

provide that service to consumers; and

3) that it is not necessary for consumers to use Plaid in order to connect their banks to the Participating Apps;

e) notify all former, current and future users of Plaid of the full scope and extent of its previous data practices and its revisions to those practices;

f) 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;

g) require, before it connects with a consumer's financial account, that the consumer review the full text of Plaid's Privacy Policy, acknowledge all of the terms and conditions by checking boxes to indicate consent to all material provisions, affirmatively agree to any collection, retention or sale of data, and acknowledge receipt and approval of the notice;

h) obtain a consumer's affirmative consent each time Plaid accesses that consumer's financial account and financial data; and

i) 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;

5. Equitable and injunctive relief enjoining Plaid from:

j) accessing, attempting to access, or procuring transmission of any consumer's identifying information through their financial accounts;

k) representing that any solicitation, request, or action by Plaid is being done by a financial institution;

l) retaining any copies, electronic or otherwise, of any identifying information obtained through the scheme alleged herein;

m) retaining any copies, electronic or otherwise, of any other information obtained from any of Plaintiff or Class Members' financial institutions using identifying information obtained through the scheme alleged herein; and

n) engaging in any unlawful activities alleged herein;

6. An order awarding Plaintiff and Class Members actual, compensatory, statutory, special and/or incidental damages as well as restitution;

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

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

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

10. Any and all other and further relief to which Plaintiff and the Classes may be entitled.

XII. DEMAND FOR JURY TRIAL

223. Plaintiff demands a trial by jury, pursuant to Federal Rule of Civil Procedure 38(b), of all issues so triable.

DATED: June 25, 2020

ROBINS KAPLAN LLP

By: /s/ *Aaron M. Sheanin*

Michael F. Ram (SBN 104805)
Aaron M. Sheanin (SBN 214472)
mram@robinskaplan.com
asheanin@robinskaplan.com
2440 W El Camino Real, Suite 100
Mountain View, CA 94040
Telephone: (650) 784-4040

Kellie Lerner (*Pro Hac Vice* to be filed)
Hollis Salzman (*Pro Hac Vice* to be filed)
William Reiss (*Pro Hac Vice* to be filed)
David Rochelson (*Pro Hac Vice* to be filed)
klerner@robinskaplan.com
hsalzman@robinskaplan.com
wreiss@robinskaplan.com
drochelson@robinskaplan.com
399 Park Avenue, Suite 3600
New York, NY 10022
Telephone: (212) 980-7400

Attorneys for Plaintiff and the Proposed Classes