1   Aaron M. Sheanin (SBN 214472)
    Christine S. Yun Sauer (SBN 314307)
2   **ROBINS KAPLAN LLP**
    2440 West El Camino Real, Suite 100
3   Mountain View, CA 94040
    Telephone: (650) 784-4040
4   Facsimile: (650) 784-4041
    asheanin@robinskaplan.com
5   cyunsauer@robinskaplan.com

6   Hollis Salzman (*pro hac vice* forthcoming)
    Kellie Lerner (*pro hac vice* forthcoming)
7   David Rochelson (*pro hac vice* forthcoming)
    ROBINS KAPLAN LLP
8   399 Park Avenue, Suite 3600
    New York, NY 10022
9   Telephone: (212) 980-7400
    Facsimile: (212) 980-7499
10 hsalzman@robinskaplan.com
    klerner@robinskaplan.com
11 drochelson@robinskaplan.com

    Christian Levis (*pro hac vice* forthcoming)
    Amanda Fiorilla (*pro hac vice* forthcoming)
    LOWEY DANNENBERG, P.C.
    44 South Broadway, Suite 1100
    White Plains, NY 10601
    Telephone: (914) 997-0500
    Facsimile: (914) 997-0035
    clevis@lowey.com
    afiorilla@lowey.com

    Anthony M. Christina (*pro hac vice* forthcoming)
    LOWEY DANNENBERG, P.C.
    One Tower Bridge
    100 Front Street, Suite 520
    West Conshohocken, PA 19428
    Telephone: (215) 399-4770
    Facsimile: (914) 997-0035
    achristina@lowey.com

12 [Additional counsel on signature page]

13

    Attorneys for Plaintiff and the Proposed Class
14

15

16   **UNITED STATES DISTRICT COURT**
                      NORTHERN DISTRICT OF CALIFORNIA

17

18   DEBORAH WESCH, individually and on behalf   Case No.:
     of all others similarly situated,

19   Plaintiff,   **CLASS ACTION COMPLAINT**

20   v.   **JURY TRIAL DEMANDED**

21   YODLEE, INC., a Delaware corporation, and
     ENVESTNET, INC., a Delaware corporation,

22   Defendants.

23

24

25

26

27

28

TABLE OF CONTENTS

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Deborah Wesch ("Plaintiff"), on behalf of herself and all others similarly situated, asserts the following against Defendants Yodlee, Inc., ("Yodlee") and Envestnet Inc., ("Envestnet") (collectively "Defendants"), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

SUMMARY OF ALLEGATIONS

1.   The Internet age has spawned the development of a vast data economy. Among its key players are data aggregators, companies that collect and repackage data from various sources for sale to advertisers, investors, researchers, and other third parties.

2.   Yodlee is one of the largest financial data aggregators in the world. Its business focuses on selling highly sensitive financial data, such as bank balances and credit card transaction histories, collected from individuals throughout the United States. For example, as Yodlee's former chief product officer explained in a 2015 interview, "'Yodlee can tell you down to the day how much the water bill was across 25,000 citizens of San Francisco,' or the daily spending at McDonald's throughout the country."[1]

3.   This data is not available from public sources and is so sensitive that the individuals it concerns would not voluntarily turn it over.

4.   Rather, Yodlee surreptitiously collects such data from software products that it markets and sells to some of the largest financial institutions in the country. These institutions, including 15 top banks (e.g., Bank of America, Merrill Lynch, and Citibank), 10 top wealth management firms, and digital payment platforms like PayPal, use Yodlee's software for various purposes, including to connect their systems to one another.

5.   Yodlee, in turn, acquires financial data about each individual that interacts with the software installed on its customers' systems. However, these individuals often have no idea they are dealing with Yodlee.

---

[1] Bradley Hope, *Provider of Personal Finance Tools Tracks Bank Cards, Sells Data to Investors,* WALL ST. J. (Aug. 6, 2015), https://www.wsj.com/articles/provider-of-personal-finance-tools-tracks-bank-cards-sells-data-to-investors-1438914620.

6.   This is by design. Given the highly sensitive nature of the data Yodlee collects, Yodlee's software is developed to be seamlessly integrated directly into the host company's existing website and/or mobile app in a way that obscures who the individual is dealing with and where their data is going. For example, when individuals connect their bank accounts to PayPal, they are prompted to enter their credentials into a log in screen that mirrors what they would see if they directly logged into their respective bank's website. *See* Part II, below. Their financial institution's logo is prominently displayed on each of the screens that they interact with and the individuals use the same usernames and passwords they would to log in to their financial institution's own website or mobile app. At no point are the individuals prompted to create or use a Yodlee account.

7.   Moreover, to the extent Yodlee is mentioned, individuals are not given accurate information about what Yodlee does or how it collects their data. For example, PayPal discloses to individuals that Yodlee is involved in connecting their bank account to PayPal's service for the limited purpose of confirming the individual's bank details, checking their balance, and transactions, as needed. While this might be true for that initial log in, Yodlee's involvement with the individual's data goes well beyond the limited consent provided to facilitate a connection between their bank account and PayPal.

8.   Yodlee, in fact, stores a copy of each individual's bank log in information (i.e., her username and password) on its own system *after* the connection is made between that individual's bank account and any other third party service (e.g., PayPal).

9.   Yodlee then exploits this information to routinely extract data from that user's accounts without their consent.

10.   This process continues even if, for example, an individual severs the connection between its bank account and the third party service (e.g., PayPal) that Yodlee facilitated. In that instance, Yodlee relies on its own stored copy of the individual's credentials to extract financial data from her accounts long after the access is revoked.

11.   This unagreed-to data collection is particularly problematic because "[c]onsumers' credit and debit card transactions can reveal information about their health, sexuality, religion,

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

political views, and many other personal details."[2] It is no wonder that Yodlee has been highly successful as, according to the *Wall Street Journal*, companies are willing to pay as much as $4 million a year for access to this sort of highly personal data.

12.   Plaintiff Deborah Wesch connected her PNC Bank account to PayPal using a Yodlee-powered portal in order to facilitate transfers among those accounts. At no time was it disclosed by PayPal, Yodlee, or PNC Bank that the Defendants would continuously access Plaintiff's bank account to extract and sell data without her consent.

13.   This is especially troubling as reports have revealed that Defendants are mishandling the data they collected from individuals without authorization by distributing it in unencrypted plain text files. These files, which can be read by anyone who acquires them, contain highly sensitive information that make it possible to identify the individuals involved in each transaction.

14.   Yodlee's failure to take even the most basic steps to protect this highly sensitive data (e.g., requiring a password to open such files) has placed Plaintiff and all Class members at significant risk of fraud and identity theft. This risk is especially heightened given Yodlee's practice of reselling the data it collects—without authorization—to third parties. While Yodlee claims to protect this data while in its custody, it has admitted in filings with the United States Securities and Exchange Commission ("SEC") that it "does not audit its customers to ensure that they have acted, and continue to act, consistently with such assurances."[3] Yodlee, accordingly, cannot guarantee Plaintiff or other Class members that its clients, or anyone with whom its clients share Class members' sensitive personal data, are not using such data for nefarious purposes.

15.   Given Defendants' secretive data collection practices and recent reports regarding its grossly inadequate approach to data security, Plaintiff believes that additional evidence supporting its claims will be uncovered following a reasonable opportunity for discovery.

---

[2] Letter from Senator Ron Wyden et al, Cong. of the U.S., to Joseph J. Simons, Chairman, Fed. Trade Comm'n (Jan. 17, 2020), https://www.wyden.senate.gov/imo/media/doc/011720%20Wyden%20Brown%20Eshoo%20Envestnet%20Yodlee%20Letter%20to%20FTC.pdf.

[3] *Proxy Statement/Prospectus*, YODLEE (Oct. 21, 2015), https://www.sec.gov/Archives/edgar/data/1337619/000104746915007906/a2226277z424b3.htm.

JURISDICTION AND VENUE

16.   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. This Court has supplemental jurisdiction over all other claims pursuant to 28 U.S.C. § 1367(a).

17.   This Court also has jurisdiction over the subject matter of this action pursuant to 28 U.S.C §1332(d), because the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, there are more than 100 putative class members defined below, and a significant portion of putative class members are citizens of a state different from Defendants.

18.   This Court has general personal jurisdiction over Yodlee because Yodlee's principal place of business is in Redwood City, California.

19.   This Court has specific personal jurisdiction over Envestnet because it regularly conducts business in this District and a substantial portion of the events and conduct giving rise to Plaintiff's claims occurred in this State.

20.   Venue is proper in this District pursuant to 28 U.S.C. §1391(b), (c), and (d) because Defendants transact business in this District; a substantial portion of the events giving rise to the claims occurred in this District; and because Defendant Yodlee is headquartered in this District.

21.   Intra-district Assignment: A substantial part of the events and omissions giving rise to the violations of law alleged herein occurred in the County of San Mateo, and as such, this action may be properly assigned to the San Francisco or Oakland divisions of this Court pursuant to Civil Local Rule 3-2(c).

PARTIES

A.   PLAINTIFF

22.   Plaintiff Deborah Wesch ("Plaintiff") is a natural person and citizen of the State of New Jersey and a resident of Monmouth County.

23.   Plaintiff Ms. Wesch is a PayPal user who connected her bank account to PayPal through Yodlee's account verification application programming interface ("API"). Defendants abused their access to Ms. Wesch's bank account by collecting and selling Plaintiff Wesch's

4

1 sensitive personal data without her knowledge or consent.

2 **B.   DEFENDANT**

3 24.   Defendant Yodlee, Inc. is a Delaware corporation with principal executive offices

4 located at 3600 Bridge Parkway, Suite 200, Redwood City, CA 94065.

5 25.   Defendant Envestnet, Inc. is a Delaware corporation, with principal executive offices

6 located at 35 East Wacker Drive, Suite 2400, Chicago, Illinois 60601.

7 <u>**FACTUAL BACKGROUND**</u>

8 **I.   THE FOUNDING OF YODLEE**

9 26.   Yodlee was founded in 1999. Initially, Yodlee was focused on providing banks and

10 financial institutions with software that would improve the user experience, for example, making it

11 possible for banking clients to view bank statements, financial accounts, and investment portfolios

12 all at once without relying on multiple logins or webpages.

13 27.   Yodlee later expanded its business to develop APIs for financial apps and software

14 (collectively, "FinTech Apps"). This includes payment apps, such as Paypal; personal budgeting

15 apps, such as Personal Capital; and apps for particular banks. Yodlee's software silently integrates

16 into its clients' existing platforms to provide various financial services, like budgeting tools, savings

17 trackers, or account history information. In each instance, the customer believes that it is interacting

18 with its home institution (e.g., its bank) and has no idea it is logging into or using a Yodlee product.

19 28.   Defendants profit from these interactions in two ways. First, the financial institutions

20 that use Defendants' software pay a licensing fee to integrate Yodlee's API into their platform.

21 Second, Yodlee collects the financial data of each individual that connects to one of the FinTech

22 Apps through a bank or other financial institution using its software. This information, which

23 includes bank account balances, transaction history and other data, is then aggregated with that of

24 other individuals and sold to third parties for a fee.

25 29.   Yodlee's reach and the amount of data it collects is extraordinary. More than 150

26 financial institutions and a majority of the 20 largest U.S. banks integrate Defendants' API into their

27 platforms. According to filings with the SEC, more than 900 companies subscribe to the Yodlee

28 platform to power customized FinTech Apps and services for millions of their users.

30.   Given its widespread success, Yodlee went public on NASDAQ in October of 2014, generating almost $100 million that year. Prior to its public offering, Yodlee claims it only provided data to third parties for "research uses," such as "enhanc[ing] predictive analysis."

31.   In 2015, Yodlee was acquired by Envestnet. The deal valued Yodlee at $590 million or approximately $19 per share. The acquisition was considered the second largest FinTech deal in U.S. history at the time.

32.   That same year, the *Wall Street Journal* released a report revealing for the first time that a large part of Yodlee's revenue was actually generated by a different lucrative source: selling user data. The report concluded that Yodlee has been selling data it gathers from users for at least the last year.

33.   Yodlee denied the *Wall Street Journal* report, claiming it had only "a very limited number of partnerships with firms to develop . . . sophisticated analytics solutions." Yodlee claimed these partners only received "a small, scrubbed, de-identified, and dynamic sample of data to enable trend analysis. Yodlee does not offer, nor do partners receive, raw data."

34.   Currently, Defendants sell sensitive personal data of tens of millions of individuals to a large customer base, including investment firms and some of the largest banks in the United States, like J.P. Morgan.[4] One of Yodlee's products, called its "Data Platform," offers "the best and most comprehensive financial data at massive scale across retail banking, credit, and wealth management." Yodlee explains "[t]his is made possible through the strengths of our data acquisition capabilities, extensive data cleaning and enrichment expertise, and massive scale."[5]

35.   Defendants' sale of users' highly sensitive personal data violates their privacy rights and several state and federal laws because, as explained below, that data is collected without Plaintiff's and Class members' knowledge or consent. Furthermore, Yodlee fails to implement

---

[4] Joseph Cox, *Leaked Document Shows How Big Companies Buy Credit Card Data on Millions of Americans*, VICE, (Feb. 19, 2017), https://www.vice.com/en_us/article/jged4x/envestnet-yodlee-credit-card-bank-data-not-anonymous.

[5] *Id.*

1 adequate security measures to protect Plaintiff's and Class members' data, leaving their highly

2 sensitive personal data vulnerable to hackers, criminals, and other unauthorized third parties.

3 **II.   YODLEE COLLECTS AND SELLS INDIVIDUALS' FINANCIAL DATA WITHOUT THEIR CONSENT**

4

5 36.   While Yodlee claims that it only sells "small . . . sample[s] of data,"[6] in reality,

6 Defendants sell millions of users' sensitive personal data to hundreds of clients. As explained below,

7 this data is collected without the individual's consent by leveraging credentials provided to Yodlee

8 for a different, specific, and limited purpose.

9 37.   For example, PayPal uses Yodlee's account verification API to validate an

10 individual's bank account so that the individual can use that account with PayPal's services. An

11 individual is prompted by the following screen when attempting to connect her bank account:

FIGURE 1

12
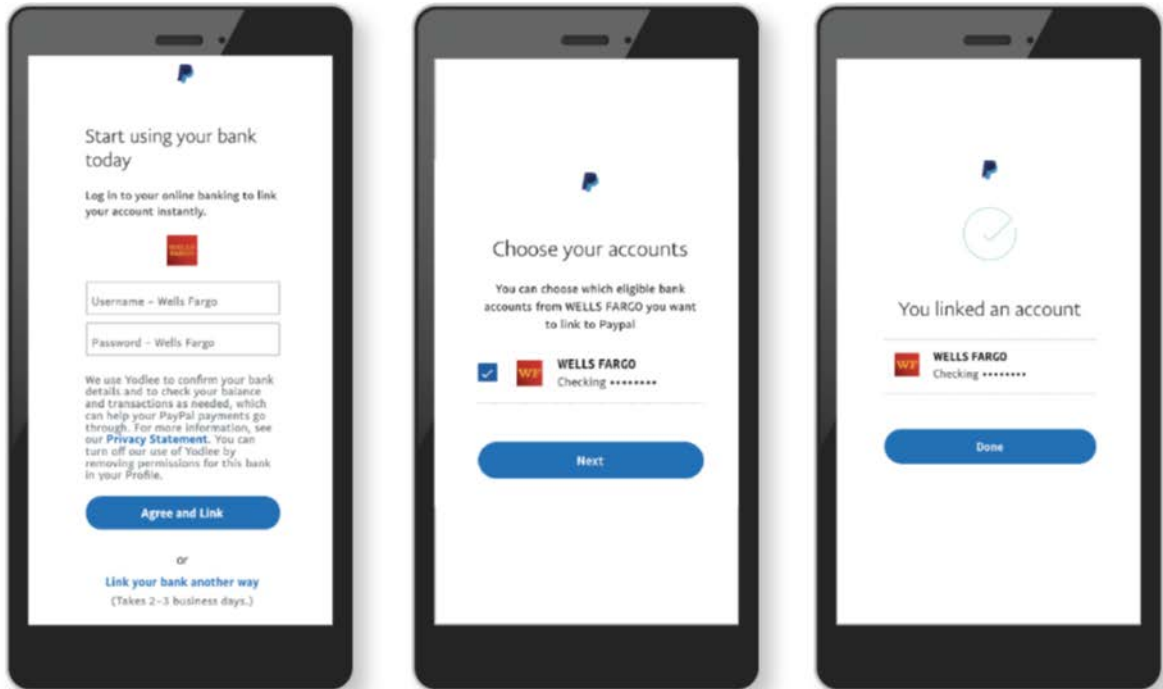
13

14

15

16

17

18

19

20

21

22

23

24 38.   The first screen displayed in Figure 1 states that "[PayPal] use[s] Yodlee to confirm

25

26 _____

27 [6] *Yodlee Responds and Corrects The Wall Street Journal Article*, YODLEE, archived at:
https://web.archive.org/web/20150816230052/https://www.yodlee.com/yodlee-responds/ (last

28 visited Aug. 21, 2020).

7

1 your bank details and to check your balance and transaction as needed, which can help your PayPal

2 payments go through." This limited interaction is all that the individual consents to. Nowhere does

3 she give either PayPal or Yodlee permission to collect and store data for resale.

4   39.   But this is exactly what happens. Yodlee goes beyond facilitating the log in

5 transactions by storing a copy of the individual's banking data, and retains the username and

6 password that the individual provides on log in screens, like that displayed in Figure 1, to collect

7 and store the individual's bank account transaction history on an ongoing basis. The individual never

8 consents to this kind of data collection, which solely benefits Yodlee and is unrelated and

9 unnecessary to complete the log in transaction.

10   40.   An individual cannot opt out of or turn off Yodlee's access to her bank account

11 information after providing her credentials. For example, while the first screen in Figure 1 states,

12 "[y]ou can turn off our use of Yodlee by removing permissions for this Bank in your Profile," this

13 pertains only to PayPal's access. Yodlee still retains the individual's credentials and continues to

14 access her bank account to collect and sell highly sensitive financial data without consent even after

15 PayPal's permissions are removed.

16   41.   Yodlee's recurring collection of and continued access to an individual's financial

17 data is never disclosed. Yodlee's privacy policy only applies to its own direct-to-consumer products

18 and does not cover the APIs that power FinTech Apps or facilitate log in transactions like that

19 described in Figure 1.[7] Instead, Yodlee directs an individual using "Yodlee powered services

20 delivered through a Yodlee client" to refer to Defendants' "client's data governance and privacy

21 practices." Thus, where an individual unknowingly uses Yodlee to connect her bank accounts to a

22 FinTech App, there is nowhere she could have looked in *Yodlee's* policies to learn the full extent of

23 data Defendants were collecting from her or the fact that Defendants were selling her data.

24   42.   Nor does Yodlee require its FinTech App clients to make any such disclosures. For

25 example, while the PayPal Privacy Statement linked to in the first screen of Figure 1 discloses that

26
---

27 [7] *Privacy Notice*, YODLEE (July 31, 2020), https://www.yodlee.com/europe/legal/privacy-notice#:~:text=The%20Yodlee%20Services%20databases%20are,of%20identification%20includi

28 ng%20biometric%20authentication.

1 PayPal does not "sell [individuals'] personal data," it says nothing about whether third-party service

2 providers, such as Yodlee, collect and sell such sensitive financial data. Likewise, while the PayPal

3 Privacy Statement provides that "you *may* be able to manage how your personal data is collected,

4 used, and shared by [third-parties]," it does not provide individuals with a way to manage what data

5 Defendants collect about them through PayPal or how Defendants use and share that data with

6 others. Such controls would have to come directly from Yodlee, which does not allow individuals

7 to manage their personal data, because doing so would undermine Defendants' highly profitable

8 data aggregation business.

9   43.   Not only do Defendants collect more data than is necessary from individuals that

10 interact with their FinTech Apps—Defendants' service is not necessary at all.

11   44.   Historically, in order to allow a third party access to a bank account, a user had to

12 submit her bank routing and account numbers; transfer a small trial deposit (usually a few cents);

13 and then return to the bank to verify the amount transferred. This process usually took several days,

14 a delay that could—in the fast-moving Internet age—cause potential users of FinTech Apps to give

15 up on using the app at all.

16   45.   One alternative to this process is "OAuth." Users are likely familiar with this

17 procedure because it has become the industry-standard protocol for users who wish to grant a

18 website or an app permission to access certain information from another website or app. Crucially,

19 OAuth "enables apps to obtain limited access (scopes) to a user's data without giving away a user's

20 password."[8] For instance, consider an example in which a user wishes to grant Facebook permission

21 to access her Twitter account so that it can integrate its social media accounts together. Before it can

22 do so, the user will be redirected from Facebook to Twitter, where it must login to ensure it is

23 authorized to grant those permissions.[9] Then, a dialogue box pops up, asking which permissions the

24 user is granting and which it is denying. The dialogue box might look something like this:

25

26 [8] *See* Matt Raible, *What the Heck is Oauth?* OKTA (June 21, 2017),
27 https://developer.okta.com/blog/2017/06/21/what-the-heck-is-oauth.

    [9] Redirection from the app the user is currently using to the app where it retains the data to which
28 it is granting permission is a hallmark of OAuth.

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL
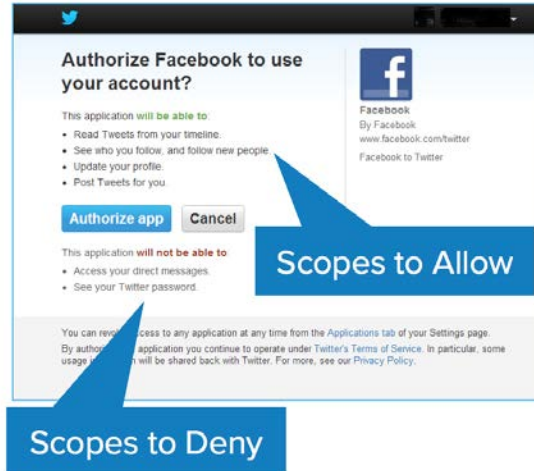
10

46.   In this example, note that the user grants Facebook permission to update its Twitter 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.

47.   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 requires a user to leave the app and be redirected to another site or interface to log in. This supposedly undermines an app's ability to sign up new users by driving away individuals who decide it is not worth the trouble of dealing with the OAuth process.

48.   Yodlee's API purports to solve this problem, but the distinctions between Yodlee's API and true OAuth underscore the grave risk that Yodlee poses to individuals. *First*, Yodlee does not provide a clear dialogue box outlining the scopes of the permissions that the user is granting to Yodlee or the permissions the user is denying to Yodlee. Indeed, the user has no option to deny Yodlee any permissions at all.

---

[10] Raible, *supra* n. 8.

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

49.   *Second*, the core principle of OAuth—and what has made it the industry-standard authorization protocol—is that it provides for access to an individual's data *without disclosing the individual's password* to the service requesting authorization. This places the individual in control, because she can cut off the service's access to her data by revoking the service's OAuth access. Yodlee specifically designed its API to circumvent this protection, deceiving users into providing Defendants with their bank usernames and passwords so that Defendants can use those credentials to collect sensitive financial information on an ongoing basis without giving the individual a way to revoke access to that data. As explained above, Defendants accomplish this by deceiving users into thinking that they are logging into their financial institutions' app or website, when in fact they are entering their credentials directly into Defendants' portal.

50.   Yodlee is capable of integrating OAuth into its API. It has done so in Europe in order to comply with the European Union's Second Payment Services Directive. Yet in the United States, Defendants continue to deploy credential-based authentication because, though it falls short of the industry standard, it is a source of immense profit.

51.   By failing to provide disclosures or obtain users' consent to collect and sell their sensitive personal data, Defendants violated Plaintiff's and Class members' privacy rights and state and federal law.

III.   YODLEE'S FAILURE TO DISCLOSE VIOLATES SEVERAL PRIVACY LAWS

52.   As discussed above, Yodlee's privacy policy only applies to its "direct-to-consumer services and websites." For consumers who access Yodlee's services through one of Yodlee's clients, such as Paypal, Yodlee pushes off the burden of providing adequate disclosures to consumers onto the client. This is an abdication of Defendants' duties under the law.

53.   In California, several statutes require Defendants to provide clear disclosures to consumers about their conduct, including that they collect and sell consumers' sensitive personal data.

54.   For example, the California Consumer Privacy Act ("CCPA") protects consumers' personal information from collection and use by businesses without providing proper notice and obtaining consent.

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

55.   The CCPA applies to Defendants Envestnet and Yodlee because they individually earn more than $25 million in annual gross revenue. Additionally, the CCPA applies to Defendants because they buy, sell, receive, or share, for commercial purposes, the personal information of more than 50,000 consumers, households, or devices.

56.   The CCPA requires a business that collects consumers' personal information, such as Defendants' business, to disclose either "at or before the point of collection . . . the categories of personal information to be collected and the purposes for which the categories of personal information shall be used." Cal. Civ Code § 1798.100(b).

57.   Furthermore, "[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." *Id.*

58.   Other state statutes that govern Defendants' disclosures include California's Financial Information Privacy Act ("CalFIPA"), Cal. Fin. Code §4053(d)(1), the California Online Privacy Protection Act ("CalOPPA"), Cal. Bus. & Prof. Code § 22575. CalFIPA 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. *See infra.*

59.   CalOPPA requires that an operator of any online service, as defined therein, "conspicuously post" its privacy policy. Cal. Bus. & Prof. Code §22575. Under the statute, to "conspicuously post" a privacy policy via a text hyperlink, the hyperlink must include the word "privacy," be "written in capital letters equal to or greater in size than the surrounding text," or be "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).

1   60.   The Graham Leach Bliley Act (the "GLBA") and the regulations promulgated

2   thereunder impose strict requirements on financial institutions regarding their treatment of

3   consumers' private financial data and the disclosure of their policies regarding the same. Defendants

4   are financial institutions subject to those regulations, which include the Privacy of Consumer

5   Financial Information regulations (the "Privacy Rule"), 16 C.F.R. Part 313, re-codified at 12 C.F.R.

6   Part 1016 ("Reg. P"), and issued pursuant to the GLBA, 15 U.S.C. §§ 6801-6803, and the GLBA's

7   "Safeguards Rule" (16 C.F.R. Part 314).

8   61.   This regulatory scheme has clear requirements for applicable privacy policies. Under

9   those rules, a financial institution "must provide a clear and conspicuous notice that accurately

10   reflects [its] privacy policies and practices." 16 C.F.R. § 313.4. Privacy notices must be provided

11   "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12

12   C.F.R. § 1016.9. "Clear and conspicuous means that a notice is reasonably understandable and

13   designed to call attention to the nature and significance of the information in the notice." 16 C.F.R.

14   § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). Ways a company can call attention to its privacy policy

15   include "[using] a plain-language heading" (16 C.F.R. §313.3(b)(2)(ii)(A); "[using] a typeface and

16   type size that are easy to read" (16 C.F.R.§ 313.3(b)(2)(ii)(B)); (c) "[using] boldface or italics for

17   key words" (16 C.F.R. § 313.3(b)(2)(ii)(D)); or (d) "[using] distinctive type size, style, and graphic

18   devices, such as shading or sidebars," when combining its notice with other information (16 C.F.R.

19   § 313.3(b)(2)(ii)(E)). A company must ensure that "other elements on the web site (such as text,

20   graphics, hyperlinks, or sound) do not distract attention from the notice." 16 CFR §313(b)(2)(iii).

21   The notice should appear in a place that users "frequently access." 16 CFR §313.3(b)(2)(iii)(A), (B).

22   Privacy notices must "accurately reflect[]" the financial institution's privacy policies and practices.

23   16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. The notices must include the

24   categories of nonpublic personal information the financial institution collects and discloses, the

25   categories of third parties to whom the financial institution discloses the information, and the

26   financial institution's security and confidentiality policies. 16 C.F.R.§ 313.6; 12 C.F.R. § 1016.6.

27   62.   Both GLBA and CalFIPA require that privacy policies provide consumers with an

28   opportunity to opt out of the sharing of their personal data. 16 C.F.R. § 313.10; Cal. Fin. Code.

1   §4053(d)(2).

2   63.   Defendants violated these statutory and regulatory requirements because they do not

3   disclose through the Yodlee privacy policy that they collect consumers' personal information, let

4   alone the categories of personal information they collect, nor the purposes for which this information

5   is collected.

6   64.   Yodlee's privacy policy is not "clear and conspicuous." Indeed, Yodlee has designed

7   its privacy policy to be wholly inapplicable to consumers like Plaintiff and Class members, who

8   access Yodlee's services through a third party.

9   65.   Nor does Yodlee make these necessary disclosures at the "point of collection." For

10 example, as discussed above, when consumers connect their bank account to PayPal through

11 Yodlee, nowhere is it disclosed that Yodlee collects and sells consumers' sensitive personal data.

12 All that is disclosed is that "[PayPal] use[s] Yodlee to confirm your bank details and to check your

13 balance and transaction as needed, which can help your PayPal payments go through." This is

14 materially false and misleading in that it does not disclose: (1) that Yodlee collects and sells users'

15 sensitive personal data; (2) the categories of data that Yodlee collects and sells; or (3) the true

16 purpose for Yodlee's conduct, i.e., to earn monetary compensation by selling Plaintiff's and Class

17 members' data to other entities. (Other apps that incorporate the Yodlee API, such as Personal

18 Capital, do not disclose their use of Yodlee whatsoever.)

19   66.   Further, Yodlee's privacy policy provides an insufficient opportunity to opt out,

20 including because it fails to use the heading "Restrict Information Sharing With Other Companies

21 We Do Business With To Provide Financial Products And Services." Cal. Fin. Code 4053 (d)(1)(A).

22   67.   In addition to being financial institutions themselves, governed by the GLBA and

23 CalFIPA, Defendants also received data from other financial institutions. As such, they violated the

24 following CalFIPA provision as well:

25   *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*
26   *ordinary course of business* to carry out the activity covered by the exception under
            which the information was received.

27

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

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

68.   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 Yodlee can *only* use such information to carry out the activity *for which the user provided consent*. Defendants' use of the data for any reason other than connecting users' bank accounts violates this statutory protection.

IV.   GOVERNMENT AND INDUSTRY LEADERS AGREE THAT DEFENDANTS' CONDUCT IS WRONG, RISKY, DANGEROUS AND BAD FOR CONSUMERS

69.   Government and industry leaders agree that Defendants' conduct runs afoul of basic standards of decency and proper treatment of consumer data.

70.   The Consumer Financial Protection Bureau's 2017 Consumer Protection Principles for data aggregators like Yodlee provide that such services should not "require consumers to share their account credentials with third parties"—i.e., anyone other than the user or the bank.[11] Of course, Defendants do exactly that.

71.   Likewise, the Consumer Protection Principles provide that the data practices of a company like Yodlee 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." Defendants' disclosures were not full and effective, as described above. Defendants' data practices were likely to and did deceive Plaintiff and Class members, are overly broad, and are not consistent with consumers' reasonable expectations, because they are out of proportion to what is necessary to link financial accounts to FinTech apps.

72.   The Consumer Protection Principles also provide that data access terms must address "access frequency, data scope, and retention period." Nowhere do Defendants disclose how they access consumers' data, how much data they gather and how long they keep it—perhaps because

---

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

1   consumers would be outraged to hear the answers.

2   73.   The Consumer Protection Principles also provide that consumers must be informed

3   of any third parties that access or use their information, including the "identity and security of each

4   such party, the data they access, their use of such data, and the frequency at which they access the

5   data." Defendants do not disclose this information.

6   74.   Major financial institutions and their trade associations have also voiced concerns.

7   In April 2016, JPMorgan CEO Jamie Dimon said the bank is "extremely concerned" about "outside

8   parties," including "aggregators" (like Yodlee), for three reasons: first, "[f]ar more information is

9   taken than the third party needs in order to do its job"; second, "[m]any third parties sell or trade

10 information in a way [users] may not understand, and the third parties, quite often, are doing it for

11 their own economic benefit – not for the customer's benefit"; and third, "[o]ften this is being done

12 on a daily basis for years after the customer signed up for the services, which they may no longer

13 be using."[12] Dimon recommended that users not share their login credentials with third parties like

14 Yodlee, in part to avoid loss of important indemnification rights: "When [users] give out their bank

15 passcode, they may not realize that if a rogue employee at an aggregator uses this passcode to steal

16 money from the customer's account, the customer, not the bank, is responsible for any loss. . . . This

17 lack of clarity and transparency isn't fair or right." JPMorgan hit the nail on the head in identifying

18 the egregious invasions of privacy that are not simply incidental to Defendants' business, but lie at

19 the heart of it.

20   75.   In 2017, the American Bankers Association ("ABA") wrote to the CFPB to express

21 similar concerns.[13] The ABA stated that "few consumers appreciate the risks presented when they

22 provide access to financial account data to non-bank fintech companies," including the risk of

23 removing such data from the secure bank environment; that "consumers are not given adequate

24

---

25 [12] *See* Jamie Dimon, Chairman and CEO of JPMorgan Chase & Co., Letter to Shareholders, (Apr.
26 6, 2016), https://www.jpmorganchase.com/corporate/annual-report/2015/.

    [13] Rob Morgan, Vice President, Emrging Techonologies of American Bankers Association, Letter
27 Response to Request for Information Regarding Consumer Access to Financial Records Docket
    No.: CFPB-2016-0048 (Feb. 21, 2017), https://www.aba.com/-/media/documents/comment-
28 letter/aba-comment-cfpb-data-aggregators.pdf?rev=a5603ffb382c49059ebab1dfda631abf.

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

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 Yodlee 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."

INJURY AND DAMAGES TO THE CLASS

76. Plaintiff and Class members have suffered actual harm, injury, damage and loss as a result of Defendants' 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 Defendants' data practices, they would not have used Yodlee.

I.   PLAINTIFF AND CLASS MEMBERS HAVE SUFFERED ECONOMIC DAMAGES

77. Defendants' 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.

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

79. Under federal regulations, a consumer is not liable for unauthorized electronic fund transfers from her financial accounts, subject to certain limits and conditions. *See, e.g.*, 12 C.F.R. § 1005.2(m). But Defendants' conduct eliminates consumers' rights to indemnification under these regulations. If Defendants induced Plaintiff and Class members to provide their bank credentials to Defendants, 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 Defendants. As noted above,

1   JPMorgan has expressed concern that consumers do not generally understand that they will be

2   responsible for any such loss. For instance, a theft of $10,000 from a consumer's account would

3   ordinarily leave a consumer liable for only $50; but if Defendants' conduct in any way contributes

4   to that unlawful access, the consumer may now be liable for the full $10,000, a loss in value of

5    $9,950. By removing Plaintiff's and Class members' data from the secure bank environment and

6   storing it in their own computer systems, networks or servers, Defendants have destroyed the rights

7   and protections to which Plaintiff and Class members are otherwise entitled. That amounts to an

8   economic loss to Plaintiff and Class members.

9   **II.   LOSS OF CONTROL OVER VALUABLE PROPERTY**

10   80.   The data that Defendants collect, retain and sell has enormous value both to

11   Defendants and to the Plaintiff and Class members from whom Defendants illicitly obtain it. First,

12   the data at issue is valuable to Defendants. In 2015, Envestnet announced an acquisition of Yodlee

13   for $590 million, based in no small part on the universe of consumer data that Yodlee had

14   accumulated. Defendants package and sell the data it collects to third party customers, thus

15   demonstrating that there is an active market for Plaintiff's and Class members' data. The sheer size

16   of this mountain of data, as well as Defendants' ability to continue accessing Plaintiff's and Class

17   members' transaction histories on an ongoing basis, creates a competitive advantage that Defendants

18   may exercise over their competitors. All of these facts indicate that the data Defendants gather is

19   valuable. Once Defendants acquire the data, however, Plaintiff and Class members have no control

20   over what Defendants do with it, including how they package it and to whom they sell it. Further,

21   even Defendants exercise no oversight or control over this data after they sell it. Thus, Plaintiff and

22   Class members suffered economic loss from the loss of control over their valuable property.

23   **A.   INCREASED RISK OF IDENTITY THEFT AND FRAUD**

24   81.   Defendants' conduct not only destroyed Plaintiff's and Class members' rights to

25   indemnification in the event their accounts are compromised, but has also increased the risk of just

26   such an incident occurring. As the ABA has recognized, the "sheer volume and value of the

27   aggregated data" warehoused at entities like Defendants makes them "a priority target for criminals,

28   including identity thieves." Databases like Defendants' create a one-stop shop for such malicious

18

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

B.   PLAINTIFF AND CLASS MEMBERS HAVE A REASONABLE EXPECTATION OF PRIVACY

82.   Plaintiff's and Class members' expectation of privacy in their highly sensitive personal data, which Defendants collected, sold, or otherwise misused, is enshrined in California's Constitution. Article I, section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, *and privacy*." Art. I., Sec. 1, Cal. Const. (emphasis added).

83.   The phrase "*and privacy*" was added in 1972 after a proposed legislative constitutional amendment designated as Proposition 11. Significantly, the argument in favor of Proposition 11 reveals that the legislative intent was to curb businesses' control over the unauthorized collection and use of consumers' personal information, stating in relevant part:

> **The right of privacy is the right to be left alone.** *It is a fundamental and compelling interest. It protects* **our homes***, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion, and our freedom to associate with the people we choose.* **It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us.**

> **Fundamental to our privacy is the ability to control circulation of personal information.** *This is essential to social relationships and personal freedom. The proliferation of government and business records over which we have no control limits our ability to control our personal lives. Often we do not know that these*

records even exist and we are certainly unable to determine who has access to them.[14]

84.   Consistent with the language of Proposition 11, numerous studies examining the collection of consumers' personal data confirm that the surreptitious taking of personal, confidential, and private information from millions of individuals, as Yodlee has done here, violates expectations of privacy that have been established as general social norms.

85.   Privacy polls and studies uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its users' personal data.

86.   For example, a recent study by *Consumer Reports* shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing their data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them. Moreover, according to a study by *Pew Research*, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.

87.   Defendants failed to disclose that they collected, sold, and otherwise misused consumers' sensitive personal data, and failed to obtain consent to do so. This constitutes a violation of Plaintiff's and Class members' privacy interests, including those enshrined in the California Constitution.

III.   YODLEE DOES NOT HAVE ADEQUATE SAFEGUARDS TO PROTECT CONSUMERS' DATA

88.   Yodlee claims that "[p]rotecting the personal information of those who use our services is [their] top priority" and that it employs "leading industry standards of de-identification processing," and "technical, administrative, and contractual measures to protect consumers' identities, such as prohibiting analytics and insights users from attempting to re-identify any

---

[14] Ballot Pamp., Proposed Amends. to Cal. Const. with arguments to voters, Gen. Elec. (Nov. 7, 1972) at 27 (emphasis added).

1   consumers from the data."[15] These statements are false.

2   89.   According to leaked documents obtained by *Vice* news, Yodlee's data anonymization

3   process involves "removing names, email addresses, and other personally identifiable information

4   (PII) from the transaction data.[16] This includes "masking patterns of numbers such as account

5   numbers, phone numbers, and SSNs and replacing them with "XXX" symbols" and "mask[ing] the

6   financial institution's name in the transaction description."[17]

7   90.   However, Yodlee's customers (and potential identify thieves) still receive a wealth

8   of information that can be used to re-identify an individual. For example, even Yodlee's "masked"

9   information still provides a unique identifier for who made the purchase, the amount of the

10   transaction, date of sale, the city, state and zip code of the business where the purchase was made,

11   and other metadata, including primary and secondary merchant fields, that can be combined to

12   identify the specific individual involved in each transaction.

13   91.   Moreover, because Yodlee keeps a unique identifier for each individual consumer in

14   its data set, and these identifiers are preserved across all transactions, marketers (and cybercriminals)

15   can de-anonymize the data by linking multiple transactions by the same user and combining that

16   information with other publicly available data.

17   92.   As Yves-Alexandre de Montjoye, an assistant professor at Imperial College London

18   explained, this data is mere "pseudonymized" than anonymized, meaning that while "it doesn't

19   contain information that'd directly identify a person such as names or email addresses . . . someone

20   with access to the dataset and some information about you . . . might be able to identify you."

21   93.   Vivek Singh, an assistant professor at Rutgers University raised the same concern,

22   because the data "does not remove spatio-temporal traces of people that can be used to connect back

23   the data to them." Spatio-temporal traces are metadata associated with the transaction, including the

24

25

[15] *See* VICE, *supra* n. 4.

26   [16] *Id.*

27   [17] *Id.*

28

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

1   data, merchant, and physical location.

2   94.   Singh and de Montjoye authored a 2015 study published in Science in which they

3   successfully identified individuals using a dataset of similar "de-identified" data using three months

4   of transactions covering 1.1 million people.[18] Singh explained with just "three to four" transactions,

5   an attacker "can unmask the person with a very high probability." The study concluded that it was

6   possible to determine the identity of an individual from so-called "anonymized" credit card data

7   90% of the time through simple extrapolation.[19]

8   95.   Significantly, last year, scientists from the Imperial College London and Université

9   Catholique de Louvain reported that they have developed a model that can re-identify 99.98% of

10 Americans from datasets using as few as fifteen demographic attributes. Notably, these researchers

11 have made their software code available for anyone on the internet.

12   96.   Consumers whose information is collected and sold by Yodlee are especially

13 vulnerable because a user's credit and debit card transactions can reveal a wealth of other personal

14 and demographic information, such as health, sexuality, religion, and political views that can be

15 used to re-identify individuals like Plaintiff and Class members.

16   97.   These studies confirm that Yodlee's purported "deanonymization" provides little to

17 no protection for Plaintiff and Class members, given the immense amount of data that Yodlee has

18 been able to collect through its network of over 17,000 connections to financial institutions, billers,

19 reward networks, and other endpoints. As Yodlee's former chief product officer Peter Hazlehurst

20 explained, Yodlee's datasets are incredible in size and "can tell you down to the day how much the

21 water bill was across 25,000 citizens of San Francisco or the daily spending at McDonald's

22 throughout the country."[20]

23

24 _____

25 [18] Y. de Montjoye, V. Singh et al., *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, 357 SCIENCE 6221, 536-539 (Jan. 30, 2015), https://science.sciencemag.org/content/347/6221/536?mod=article_inline.

26 [19] *Id.*

27 [20] Hope, *supra* n.1.

28

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

98.   Furthermore, despite Yodlee's claim that it employs "technical, administrative, and contractual measures to protect consumers' identities, such as prohibiting analytics and insights users from attempting to re-identify any consumers from the data,"[21] Yodlee does not have reasonable safeguards in place to protect consumers' sensitive personal data.

99.   Yodlee admitted in a 2015 filing with the SEC that it "does not audit its customers to ensure that they have acted, and continue to act, consistently with such assurances."[22] After selling consumer data, Yodlee takes no steps to ensure this information remains private, that its clients are not attempting to re-identify consumers, or use that data for malicious purposes.

100.   Nor could it. Yodlee's choice not to employ technical safeguards to protect consumers' sensitive personal data and instead to sell that data to its clients in large text files removes Yodlee's ability to exert any control over the information once it has been sold.

IV.   CONGRESS HAS REQUESTED AN FTC INVESTIGATION INTO ENVESTNET & YODLEE PRACTICES

101.   Earlier this year, three members of Congress wrote a letter urging the Federal Trade Commission ("FTC") to investigate Defendants for selling Americans' highly sensitive data without their knowledge or consent.[23]

102.   In the letter, Senator Ron Wyden, Senator Sherrod Brown, and Representative Anna Eshoo wrote that "Envestnet [] sells access to consumer data . . . The consumer data that Envestnet collects and sells is highly sensitive. Consumers' credit and debit card transactions can reveal information about their health, sexuality, religion, political views, and many other personal details . . . And the more often that consumers' personal information is bought and sold, the greater the risk that it could be the subject of a data breach."

103.   The three members of Capitol Hill were deeply worried that "Envestnet and the

---

[21] *See* Vice, *supra* n. 4.

[22] *Proxy Statement/Prospectus*, YODLEE, (Oct. 14, 2015), https://www.sec.gov/Archives/edgar/data/1337619/000104746915007906/a2226277z424b3.htm

[23] *See* Wyden, *supra* n. 2.

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

1   companies to which it had sold data [did not] have the required technical controls in place to protect

2   Americans' sensitive financial data from re-identification, unauthorized disclosure to hackers or

3   foreign spies, or other abusive data practices." [24]

4   104.   The letter further warned that:

5   Envestnet does not inform consumers that it is collecting and selling their personal
         financial data . . . Instead, Envestnet only asks its partners, such as banks, to disclose

6   this information to consumers in their terms and conditions or privacy policy. That
         is not sufficient protection for users. Envestnet does not appear to take any steps to

7   ensure that its partners actually provide consumers with such notice. And even if
         they did, Envestnet should not put the burden on consumers to locate a notice buried

8   in small print in a bank's or apps' [sic] terms and conditions . . . in order [to] protect
         their privacy.

9

10 The authors argued that FTC policy prohibits "hid[ing] important facts about how consumer data is

11 collected or shared in the small print of a privacy policy" and FTC has stated that, "companies have

12 an obligation to disclose 'facts [that] would be material to consumers in deciding to install the

13 software.'"

14   105.   According to Envestnet's most recent Form 10-K, in February 2020, the FTC issued

15 a civil investigative demand to Envestnet for various documents related to this matter. Envestnet

16 itself recognizes the risk that as a result of the FTC's investigation, proceedings may be initiated

17 and they may be found to have violated applicable laws, which could have a material adverse effect

18 on their operations and financial condition.

19   **TOLLING, CONCEALMENT AND ESTOPPEL**

20   106.   The statutes of limitation applicable to Plaintiff's claims are tolled as a result of

21 Defendants' knowing and active concealment of their conduct alleged herein. Among other things,

22 Defendants design their software to deceive users into thinking that they are interacting directly with

23 their banks when providing log in credentials to facilitate a connection between their bank accounts

24 and a third party service. Defendants also fail to disclose to each individual user—either through

25 their own privacy policy, website, or other document—that they store the bank log in information

26 provided in such log in transactions and use those credentials to collect financial data from the

27 _____

28 [24] *Id.*

1   individual's bank accounts on an ongoing basis, even though the individual never consented to such

2   data collection. Nor do Defendants inform each individual user that this data collection will continue

3   even if the individual revokes the permissions granted to the third party service it sought to connect

4   to her bank account. By these actions, Defendants intentionally concealed the nature and extent of

5   their data collection operation to maximize profits resulting from the sale of Plaintiff's and Class

6   members' highly sensitive financial information. To the extent the Defendants' customers or others

7   made statements regarding Defendants' service or its privacy policies, Defendants either approved

8   those inadequate statements or failed to timely correct them in service of their ongoing scheme to

9   conceal the true nature of their conduct.

10   107.   Plaintiff and Class members could not, with due diligence, have discovered the full

11   scope of Defendants' conduct, due to Defendants' deliberate efforts to conceal it. All applicable

12   statutes of limitation also have been tolled by operation of the discovery rule. Under the

13   circumstances, Defendants were under a duty to disclose the nature and significance of their data

14   and privacy policies and practices, but did not do so. Defendants therefore are estopped from relying

15   on any statute of limitations.

16   108.   Defendants' fraudulent concealment and omissions are common to Plaintiff and all

17   Class members.

18   **CLASS ACTION ALLEGATIONS**

19   109.   Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23

20   individually and on behalf of the following Classes:

21   **Nationwide Class:** All natural persons in the United States whose accounts at a
            financial institution were accessed by Yodlee using login credentials obtained
22   through Yodlee's software incorporated in a mobile or web-based fintech app that
            enables payments (including ACH payments) or other money transfers from 2014
23   through the present.

24   **California Class:** All natural persons in California whose accounts at a financial
            institution were accessed by Yodlee using login credentials obtained through
25   Yodlee's software incorporated in a mobile or web-based fintech app that enables
            payments (including ACH payments) or other money transfers from 2014 through

26

27

28

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

1   the present.[25]

2   110.   Excluded from each of the Classes are: (1) any Judge or Magistrate presiding over

3   this action and any members of their families; (2) Defendants, Defendants' subsidiaries, parents,

4   successors, predecessors, and any entity in which a Defendant or its parent has a controlling interest

5   and their current or former employees, officers, and directors; and (3) Plaintiff's counsel and

6   Defendants' counsel.

7   111.   **Numerosity:** The exact number of members of the Classes is unknown and

8   unavailable to Plaintiff at this time, but individual joinder in this case is impracticable. The Classes

9   likely consist of millions of individuals, and the members can be identified through Defendants'

10   records.

11   112.   **Predominant Common Questions:** The Classes' claims present common questions

12   of law and fact, and those questions predominate over any questions that may affect individual Class

13   members. Common questions for the Classes include, but are not limited to, the following:

14   a.   Whether Defendants violated Plaintiff's and Class members' privacy rights;

15   b.   Whether Defendants' acts and practices complained of herein amount to egregious

16   breaches of social norms;

17   c.   Whether Defendants' conduct was negligent;

18   d.   Whether Defendants' conduct was unlawful;

19   e.   Whether Defendants' conduct was unfair;

20   f.   Whether Defendants' conduct was fraudulent;

21   g.   Whether Plaintiff and the Class members are entitled to equitable relief, including

22   but not limited to, injunctive relief, restitution, and disgorgement;

23   h.   Whether Plaintiff and the Class members are entitled to actual, statutory, punitive or

24   other forms of damages, and other monetary relief; and

25   i.   Whether Plaintiff and the Class members are entitled to actual, statutory, punitive or

26   _____

27   [25] Plaintiff has defined the Classes based on currently available information and hereby reserves
     the right to amend the definition of the Classes, including, without limitation, the Class Period.
28

1   other forms of damages, and other monetary relief.

2   113.   **Typicality:** Plaintiff's claims are typical of the claims of the other members of the

3   Classes. The claims of Plaintiff and the members of the Classes arise from the same conduct by

4   Defendants and are based on the same legal theories.

5   114.   **Adequate Representation:** Plaintiff has and will continue to fairly and adequately

6   represent and protect the interests of the Classes. Plaintiff has retained counsel competent and

7   experienced in complex litigation and class actions, including litigations to remedy privacy

8   violations. Plaintiff have no interest that is antagonistic to those of the Classes, and Defendants have

9   no defenses unique to any Plaintiff.   Plaintiff and her counsel are committed to vigorously

10   prosecuting this action on behalf of the members of the Classes, and they have the resources to do

11   so. Neither Plaintiff nor her counsel have any interest adverse to those of the other members of the

12   Classes.

13   115.   **Substantial Benefits:** This class action is appropriate for certification because class

14   proceedings are superior to other available methods for the fair and efficient adjudication of this

15   controversy and joinder of all members of the Classes is impracticable. This proposed class action

16   presents fewer management difficulties than individual litigation, and provides the benefits of single

17   adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment

18   will create economies of time, effort, and expense and promote uniform decision-making.

19   116.   Plaintiff reserves the right to revise the foregoing class allegations and definitions

20   based on facts learned and legal developments following additional investigation, discovery, or

21   otherwise.

22   **CALIFORNIA LAW APPLIES TO THE NATIONWIDE CLASS**

23   117.   California's substantive laws apply to every member of the Nationwide Class,

24   regardless of where in the United States the Class member resides. The State of California has

25   sufficient contacts to Defendants' relevant conduct for California law to be uniformly applied to the

26   claims of the Nationwide Class.

27   118.   Further, California's substantive laws may be constitutionally applied to the claims

28   of Plaintiff and the Nationwide Class under the Due Process Clause, 14th Amend. § 1, and the Full

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

1   Faith and Credit Clause, Art. IV § 1 of the U.S. Constitution. California has significant contacts, or

2   significant aggregation of contacts, to the claims asserted by Plaintiff and all Class members, thereby

3   creating state interests that ensure that the choice of California state law is not arbitrary or unfair.

4   119.   Yodlee's headquarters and principal place of business is located in California.

5   Defendants also own property and conduct substantial business in California, and therefore

6   California has an interest in regulating Defendants' conduct under its laws. Defendants' conduct

7   originated in, and emanated from, California and impacted a significant percentage of California

8   residents, rendering the application of California law to the claims here constitutionally permissible.

9   120.   The application of California laws to the Nationwide Class is also appropriate under

10   California's choice of law rules because California has significant contacts to the claims of Plaintiff

11   and the proposed Nationwide Class, and California has a greater interest in applying its laws here

12   than any other interested state.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

Common Law Invasion of Privacy – Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Classes)

17   121.   Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with

18   the same force and effect as if fully restated herein.

19   122.   Defendants intruded upon Plaintiff and Class members' seclusion by (1) collecting,

20   retaining and selling their sensitive personal data in which they had a reasonable expectation of

21   privacy; and (2) in a manner that was highly offensive to Plaintiff and Class members, would be

22   highly offensive to a reasonable person, and was an egregious violation of social norms.

23   123.   Defendants' conduct violated Plaintiff's and Class members' interests by collecting,

24   selling, and otherwise misusing their sensitive personal data, including information concerning

25   private financial transactions (i.e., their informational privacy rights), as well as their interests in

26   making intimate personal decisions or conducting personal activities without observation, intrusion,

27   or interference (i.e., their autonomy privacy rights). Defendants' conduct is especially egregious as

28   they fail to have any adequate security measures in place to control what their clients do with

1 Plaintiff's and Class members' information once it is sold, such as re-identifying Plaintiff and Class

2 members or using it for nefarious purposes.

3   124.   The surreptitious taking and disclosure of personal, confidential, and private

4 information from millions of individuals was highly offensive because it violated expectations of

5 privacy that have been established by general social norms.

6   125.   Polls and studies consistently show that the overwhelming majority of Americans

7 believe one of the most important privacy rights is the need for an individual's affirmative consent

8 before personal data is shared. For example, one study by *Pew Research* found that 93% of

9 Americans believe it is important to be in control of who can get information about them.

10   126.   Defendants' conduct would be highly offensive to a reasonable person in that it

11 violated federal and state laws designed to protect individual privacy, in addition to social norms.

12   127.   Defendants intentionally engaged in the misconduct alleged herein for their own

13 financial benefit unrelated to any service they provide. Specifically, Defendants collected and sold

14 Plaintiff's and Class members' lucrative (and private) sensitive information for their own financial

15 benefit.

16   128.   As a result of Defendants' actions, Plaintiff and Class members have suffered harm

17 and injury, including but not limited to an invasion of their privacy rights.

18   129.   Plaintiff and Class members have been damaged as a direct and proximate result of

19 Defendants' invasion of their privacy and are entitled to just compensation.

20   130.   Plaintiff and Class members are entitled to appropriate relief, including

21 compensatory damages for the harm to their privacy and dignitary interests, loss of valuable rights

22 and protections, heightened risk of future invasions of privacy, and mental and emotional distress.

23   131.   Plaintiff and Class members are entitled to an order requiring Defendants to disgorge

24 profits or other benefits that Defendants acquired as a result of its invasions of privacy.

25   132.   Plaintiff and Class members are entitled to punitive damages resulting from the

26 malicious, willful and intentional nature of Defendants' actions, directed at injuring Plaintiff and

27 Class members in conscious disregard of their rights. Such damages are needed to deter Defendants

28 from engaging in such conduct in the future.

1   133.   Plaintiff also seeks such other relief as the Court may deem just and proper.

2   **SECOND CLAIM FOR RELIEF**

3   **Stored Communications Act ("SCA")**
    18 U.S.C. § 2701
4   **(On Behalf of Plaintiff and the Classes)**

5   134.   Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with

6   the same force and effect as if fully restated herein.

7   135.   The SCA provides that a person "providing an electronic communication service to

8   the public shall not knowingly divulge to any person or entity the contents of a communication while

9   in electronic storage by that service[.]" 18 U.S.C. § 2702(a)(1).

10   136.   "Electronic communication" is broadly defined as "any transfer of signs, signals,

11   writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire,

12   radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign

13   commerce[.]" 18 U.S.C. § 2510(12).

14   137.   "Electronic storage" is defined as "any temporary, intermediate storage of a wire or

15   electronic communication incidental to the electronic transmission thereof; and any storage of such

16   communication by an electronic communication service for purposes of backup protection of such

17   communication[.]" 18 U.S.C. § 2510(17)(A)-(B).

18   138.   "Electronic communication service" is defined as "any service which provides to

19   users thereof the ability to send or receive wire or electronic communications[.]" 18 U.S.C. §

20   2510(15).

21   139.   "Person" is defined as "any employee, or agent of the United States or any State or

22   political subdivision thereof, and any individual, partnership, association, joint stock company, trust,

23   or corporation." 18 U.S.C. § 2510(6).

24   140.   Yodlee and Envestnet, as corporations, are persons as defined under 18 U.S.C. §

25   2510(6).

26   141.   Defendants provide a service that allows Plaintiff and Class members the ability to

27   send and receive electronic communications from their financial institutions and third-party

28   applications, such as PayPal. Defendants provide this service "to the public" because Defendants'

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

1   FinTech and PFM technology is incorporated in hundreds of applications used by millions of

2   individuals, including Plaintiff and Class members.

3   142.   Plaintiff and Class members reasonably expected that Defendants' service did not

4   include accessing, collecting, selling, and otherwise disclosing their "electronic communications,"

5   i.e., their data (as broadly defined), based, in part, on Defendants' failure to provide *any* disclosures

6   or obtain consent for permission to do so.

7   143.   Defendants store Plaintiff's and Class members' electronic communications and

8   intentionally divulged them by selling this information to third parties for monetary compensation,

9   in reckless disregard for Plaintiff's and Class members' privacy rights for Defendants' own financial

10 benefit.

11   144.   Defendants' actions were at all relevant times intentional, willful, and knowing, as

12 evidenced by Defendants accepting monetary compensation in exchange for Plaintiff's and Class

13 members' electronic communications.

14   145.   As a result of Defendants' violations of the SCA, Plaintiff and Class members have

15 suffered harm and injury, including but not limited to the invasion of their privacy rights.

16   146.   Pursuant to 18 U.S.C. § 2707, Plaintiff and Class members are entitled to: (1)

17 appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial,

18 assessed as the sum of the actual damages suffered by Plaintiff and the Class and any profits made

19 by Defendants as a result of the violation, but in no case less than the minimum statutory damages

20 of $1,000 per person; and (3) reasonable attorneys' fees and other litigation costs reasonably

21 incurred.

22   **THIRD CLAIM FOR RELIEF**

23   **Unjust Enrichment**
                            (On Behalf of Plaintiff and the Classes)
24

25   147.   Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with

26 the same force and effect as if fully restated herein.

27   148.   Defendants received benefits from Plaintiff and Class members and unjustly retained

28 those benefits at their expense.

1   149.   In particular, Defendants received benefits from Plaintiff and Class members in the

2 form of the sensitive personal data that Defendants collected from Plaintiff and Class members,

3 without authorization and proper compensation. Defendants have collected, sold, and otherwise

4 misused this information, for their own gain, providing Defendants with economic, intangible, and

5 other benefits, including substantial monetary compensation from the entities who purchased

6 Plaintiff's and Class members' sensitive personal data.

7   150.   Defendants unjustly retained those benefits at the expense of Plaintiff and Class

8 members because Defendants' conduct damaged Plaintiff and Class members, all without providing

9 any commensurate compensation to Plaintiff and Class members.

10   151.   The benefits that Defendants derived from Plaintiff and Class members rightly

11 belong to Plaintiff and Class members. It would be inequitable under unjust enrichment principles

12 in California and every other state for Defendants to be permitted to retain any of the profit or other

13 benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in

14 this Complaint.

15   152.   Defendants should be compelled to disgorge in a common fund for the benefit of

16 Plaintiff and Class members all unlawful or inequitable proceeds it received, and such other relief

17 as the Court may deem just and proper.

FOURTH CLAIM FOR RELIEF

Violation of Cal. Civ. Code § 1709
(On Behalf of Plaintiff and the Classes)

21   153.   Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with

22 the same force and effect as if fully restated herein.

23   154.   California Civil Code § 1709 provides that "[o]ne who willfully deceives another

24 with intent to induce him to alter his position to his injury or risk, is liable for any damage which he

25 thereby suffers." A defendant violates §1709 if (i) it had a duty to disclose a material fact to the

26 plaintiff; (ii) it intentionally concealed that fact with intent to defraud; (iii) plaintiff was unaware of

27 that fact (and would have acted differently if he were aware), and (iv) plaintiff sustained some

28 damage as a result.

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

1   155.   California Civil Code § 1710 defines "deceit" as "1. [t]he suggestion, as a fact, of

2 that which is not true, by one who does not believe it to be true; 2. [t]he assertion, as a fact, of that

3 which is not true, by one who has no reasonable ground for believing it to be true; 3. [t]he

4 suppression of a fact, by one who is bound to disclose it, or who gives information of other facts

5 which are likely to mislead for want of communication of that fact; or, 4. [a] promise, made without

6 any intention of performing it."

7   156.   Defendants engaged in various acts of deceit. Defendants either suggested that

8 certain facts are true which they knew were not true or which they had no reasonable grounds to

9 believe were true. For example, when Plaintiff and Class members link their bank account to Paypal

10 through Yodlee, the only disclosure provided is that Yodlee is used "to confirm your bank details

11 and to check your balance and transaction *as needed*, which can help your PayPal payments go

12 through." This statement is objectively false. Yodlee accesses users' bank accounts beyond the

13 purposes that it claims. Yodlee actually accesses users' bank accounts to collect their sensitive

14 personal data and sell it to their customers, well beyond what is necessary to connect users' bank

15 accounts to PayPal.

16   157.   Furthermore, Yodlee suppresses facts and provides other facts that are likely to

17 mislead. For example, Yodlee does not inform consumers that it collects and sells their sensitive

18 personal data. Yodlee improperly relies on its clients to provide necessary disclosures of Yodlee's

19 own practices and takes no steps to ensure that its clients do so. By failing to disclose these material

20 facts, Plaintiff and Class members were deceived.

21   158.   Defendants willfully engaged in these acts of deceit with intent to induce Plaintiff

22 and Class members to alter their position to their injury or risk, namely by turning over their sensitive

23 personal data to Defendants under false pretenses.

24   159.   Defendants had a duty to disclose these facts to Plaintiff and Class members; they

25 intentionally concealed those facts with intent to defraud; Plaintiff and Class members were unaware

26 of these facts, and would have acted differently if they were aware; and Plaintiff and Class members

27 sustained damage as a result.

28   160.   Defendants willfully also engaged in these acts of deceit so that they could access,

1   collect, and sell Plaintiff's and Class members' sensitive personal data for their own personal

2   benefit, including monetary compensation.

3   161.   Plaintiff and Class members seek recovery of their resulting damages, including

4   economic damages, restitution, and disgorgement, as well as punitive damages and such other relief

5   as the Court may deem just and proper.

6   **FIFTH CLAIM FOR RELIEF**

7   **Violation of California Unfair Competition Law ("UCL")**
         Cal. Bus. & Prof. Code § 17200
8   **(On Behalf of Plaintiff and the Classes)**

9   162.   Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with

10   the same force and effect as if fully restated herein.

11   163.   Defendants' conduct as alleged herein constitutes unlawful, unfair, and/or fraudulent

12   business acts or practices as prohibited by the UCL.

13   164.   Defendants' business acts and practices are "unlawful" under the UCL, because, as

14   alleged above, Defendant violated the California common law, California Constitution, California

15   Civil Code § 1709, the California Consumer Privacy Act, and the Stored Communications Act.

16   165.   Defendants' business acts and practices are "unfair" under the UCL. California has

17   a strong public policy of protecting consumers' privacy interests, including protecting consumers'

18   banking data. Defendants violated this public policy by, among other things, surreptitiously

19   collecting, selling, and otherwise misusing Plaintiff's and Class members' sensitive personal data

20   without Plaintiff's and Class members' consent. Defendants' conduct violates the policies of the

21   statutes referenced above.

22   166.   Defendants' business acts and practices are also "unfair" in that they are immoral,

23   unethical, oppressive, unscrupulous and/or substantially injurious to consumers. The gravity of the

24   harm of Defendants' secretly collecting, selling, and otherwise misusing Plaintiff's and Class

25   members' sensitive personal data is significant, and there is no corresponding benefit resulting from

26   such conduct. Finally, because Plaintiff and Class Members were completely unaware of

27   Defendants' conduct, they could not have possibly avoided the harm.

28   167.   Defendants' business acts and practices are also "fraudulent" within the meaning of

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

1 the UCL. Defendants have amassed a large collection of sensitive personal data without complete

2 disclosure and therefore without consumers' knowledge or consent. Defendants' business acts and

3 practices were likely to, and did, deceive members of the public including Plaintiff and Class

4 members into believing this data was private and only used as necessary, such as to connect users'

5 bank accounts to third party applications. In fact, such information was not private, as Defendants

6 secretly collected, sold, and otherwise misused it for their own purposes.

7   168.   Had Plaintiff and Class members known that their information would be collected,

8 sold, and otherwise misused for Defendants' benefit, they would not have used Defendants'

9 services.

10   169.   Plaintiff and Class members have a property interest in their sensitive personal data.

11 By surreptitiously collecting, selling, and otherwise misusing Plaintiff's and Class members'

12 information, Defendants have taken property from Plaintiff and Class members without providing

13 just or any compensation.

14   170.   Plaintiff and Class members have lost money and property as a result of Defendants'

15 conduct in violation of the UCL and seek restitution on behalf of themselves and Class members.

16 Additionally, Plaintiff and Class members are entitled to an order enjoining Defendants from

17 engaging in the unlawful conduct alleged in this claim and requiring Defendants to delete Plaintiff's

18 and Class members sensitive personal data, to cease further collection of Plaintiff's and Class

19 members sensitive personal data, and other appropriate equitable relief, including but not limited to

20 improving its privacy disclosures and obtaining adequately informed consent.

21 <div align="center">**SIXTH CLAIM FOR RELIEF**</div>

22 <div align="center">**Request for Relief Under the Declaratory Judgment Act**
28 U.S.C. § 2201, *et seq.*</div>

23 <div align="center">**(On Behalf of Plaintiff and the Classes)**</div>

24   171.   Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with

25 the same force and effect as if fully restated herein.

26   172.   Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is

27 authorized to enter a judgment declaring the rights and legal relations of the parties and grant further

28 necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are

1   tortious and that violate the terms of the federal and state statutes described in this complaint.

2   173.   An actual controversy has arisen in the wake of Defendants' collection, offer for sale,

3   and other misuse of Plaintiff's and Class members' sensitive personal data without their consent as

4   alleged herein in violation of Defendants' common law and statutory duties.

5   174.   Plaintiff and Class members continue to suffer injury and damages as described

6   herein as Defendants continue to collect, sell, and misuse Plaintiff's and Class members' sensitive

7   personal data.

8   175.   Pursuant to its authority under the Declaratory Judgment Act, this Court should enter

9   a judgment declaring, among other things, the following:

10   a.   Defendants continue to owe a legal duty to not collect, sell, and misuse

11   Plaintiff's and Class members' sensitive personal information under, *inter*

12   *alia*, the common law, California Constitution, California Civil Code § 1709,

13   and the California Consumer Privacy Act.

14   b.   Defendants continue to breach their legal duties by continuing to monitor,

15   collect, and misuse Plaintiff's and Class members' sensitive personal data;

16   and

17   c.   Defendants' ongoing breaches of their legal duty continue to cause Plaintiff

18   and Class members harm.

19   176.   The Court should also issue corresponding injunctive relief, including but not limited

20   to enjoining Defendants from engaging in the unlawful conduct alleged in this complaint and

21   requiring Defendants to delete Plaintiff's and Class members' sensitive personal data, cease further

22   collection of Plaintiff's and Class members sensitive data, stop selling Plaintiff's and Class

23   members' sensitive data, and other appropriate equitable relief, including but not limited to

24   providing privacy disclosures and obtaining adequately informed consent.

25   177.   If an injunction is not issued, Plaintiff and Class members will suffer irreparable

26   injury and lack an adequate legal remedy in the event of Defendants' ongoing conduct.

27   178.   Federal and state laws prohibit, among other things, the unlawful collection, offering

28   for sale, and other misuse of sensitive personal data without consent. California specifically

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

1 recognizes privacy as a fundamental right. The risk of continued violations of federal and California

2 law is real, immediate, and substantial. Plaintiff and Class members do not have an adequate remedy

3 at law because many of the resulting injuries are reoccurring, and Plaintiff and Class members will

4 be forced to bring multiple lawsuits to rectify the same conduct.

5   179.   The hardships to Plaintiff and Class members if an injunction is not issued exceed

6 the hardships to Defendants if an injunction is issued. On the other hand, the cost to Defendants of

7 complying with an injunction by complying with federal and California law and by ceasing to

8 engage in the misconduct alleged herein is relatively minimal, and Defendants have a pre-existing

9 legal obligation to avoid invading the privacy rights of consumers.

10   180.   Issuance of the requested injunction will serve the public interest by preventing

11 ongoing monitoring, collection, and misuse of sensitive personal data without consent, thus

12 eliminating the injuries that would result to Plaintiff and the Class.

SEVENTH CAUSE OF ACTION

**Violation of California's Comprehensive Data Access and Fraud Act ("CDAFA"),
Cal. Pen. Code § 502
(On Behalf of Plaintiff and the Classes)**

16   181.   Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with

17 the same force and effect as if fully restated herein.

18   182.   Plaintiff brings this claim on behalf of herself and the Nationwide Class or, in the

19 alternative, the California Class, under California law.

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

21   184.   A person violates Cal. Penal Code § 502(c)(1) if it "*[k]nowingly accesses* and *without*

22 *permission alters, damages, destroys, or otherwise uses . . . any data*, computer, computer system,

23 or computer network in order to either (A) devise or execute any scheme or artifice to defraud,

24 deceive or extort, or (B) wrongfully control or obtain money, property or data." (Emphasis added.)

25 Defendants violated § 502(c)(1) when it accessed Plaintiff's and Class members' sensitive personal

26 information and damaged and used Plaintiff's and Class members' sensitive personal information.

27 Defendants acted without permission for the reasons described herein. Plaintiff and Class members

28 had no notice, whether actual or constructive, that Defendants were a separate entity from the

1   FinTech Apps, and thus no notice that Defendants were operating; had no way to remove

2   Defendants' software; and do not have an opportunity to consent to Defendants' access to their

3   sensitive personal data each time that Defendants access it. Defendants accessed and used this data

4   in order to execute their scheme to defraud and deceive, because Defendants employed fraud and

5   deceit to induce Plaintiff and Class members to turn over their financial institution login credentials

6   to Defendants. Additionally, Defendants accessed and used this data to wrongfully obtain money,

7   property or data, both because it obtained the data under false pretenses and because it used the data

8   to develop analytics products that it then sold.

9   185.   A person violates Cal. Penal Code § 502(c)(2) if it "*[k]nowingly accesses* and *without*

10   *permission* takes, copies, or *makes use of any data* from a computer, computer system, or computer

11   network." (Emphasis added.) Defendants violated § 502(c)(2) when they accessed Plaintiff's and

12   Class members' sensitive personal information without permission as described herein, and made

13   use of Plaintiff's and Class members' sensitive personal information without permission as

14   described herein.

15   186.   A person violates Cal. Penal Code § 502(c)(3) if it "*[k]nowingly and without*

16   *permission uses or causes to be used computer services.*" (Emphasis added.) Defendants violated

17   § 502(c)(3) when they knowingly and without permission used or caused to be used the computer

18   services of Plaintiff's and Class members' financial institutions, as described herein.

19   187.   A person violates Cal. Penal Code § 502(c)(4) if it "*[k]nowingly accesses and*

20   *without permission* adds, alters, *damages*, deletes, or destroys any data, computer software, or

21   computer programs which reside or exist internal or external to a computer, computer system, or

22   computer network." (Emphasis added.) Defendants violated § 502(c)(4) when they knowingly

23   damaged Plaintiff's and Class members' sensitive personal data, and damaged Plaintiff's and Class

24   members' financial institutions' computers, computers systems and computer networks, as

25   described herein. Defendants acted without permission for the reasons described herein.

26   188.   A person violates Cal. Penal Code § 502(c)(6) if it "*[k]nowingly and without*

27   *permission provides or assists in providing a means of accessing* a computer, computer system, or

28   computer network in violation of this section." (Emphasis added.) Defendants violated § 502(c)(6)

38

1   when they knowingly used Plaintiff's and Class members' login credentials, which they obtained

2   under false pretenses, and provided them to Plaintiff's and Class members' financial institutions, as

3   described herein. Defendants acted without permission for the reasons described herein.

4   189.   A person violates Cal. Penal Code § 502(c)(7) if it "*[k]nowingly and without*

5   *permission accesses or causes to be accessed* any computer, computer system, or computer

6   network." (Emphasis added.) Defendants violated § 502(c)(7) when they knowingly used Plaintiff's

7   and Class members' login credentials, which they obtained under false pretenses, to access the

8   computers, computer systems and computer networks of Plaintiff and Class members' financial

9   institutions, as described herein. Defendants acted without permission for the reasons described

10   herein.

11   190.   Defendants accessed the data, computers, computer systems and computer networks

12   above in ways that circumvented technical or code-based barriers.

13   191.   Plaintiff and Class members are owners of the sensitive personal data that Defendants

14   collected, retained and sold, and suffered actual harm, injury, damage and loss as a result of

15   Defendants' conduct, as described herein. Thus, Plaintiff and Class members may bring a civil

16   action for compensatory damages, including "expenditure[s] reasonably and necessarily

17   incurred . . . to verify that . . . data was or was not altered, damaged or deleted by access." Cal. Pen.

18   Code § 502(e)(1). Further, Defendants shall pay punitive and/or exemplary damages because their

19   violations were willful. *Id.* § 502(e)(4). Plaintiff shall be entitled to reasonable attorney's fees. *Id.*

20   § 502(e)(2). Plaintiff also seeks such other relief as the Court may deem just and proper.

21   **EIGHTH CAUSE OF ACTION**

22   **Violation of California's Anti-Phishing Act of 2005**
    Cal. Bus. & Prof. Code § 22948.2
23   **(On Behalf of Plaintiff and the Classes)**

24   192.   Plaintiff incorporates the substantive allegations contained in all prior and

25   succeeding paragraphs as if fully set forth herein.

26   193.   Plaintiff brings this claim on behalf of herself and the Nationwide Class or, in the

27   alternative, the California Class.

28   194.   The California Anti-Phishing Act of 2005 (the "Anti-Phishing Act") makes it

1   unlawful to use the Internet "to solicit, request, or take any action to induce another person to provide

2   identifying information by representing itself to be a business without the authority or approval of

3   the business." Cal. Bus. & Prof. Code § 22948.2. "Identifying information" includes bank account

4   numbers, account passwords, and "[a]ny other piece of information that can be used to access an

5   individual's financial accounts." Cal. Bus. & Prof. Code § 22948.1(b). An individual who is

6   adversely affected by a violation of Section 22948.2 may bring an action. Cal. Bus. & Prof. Code

7   § 22948.3(a)(2).

8   195.   As described herein, Defendants violated the Anti-Phishing Act by representing

9   themselves to be Plaintiff's and Class members' financial institutions. Defendants fraudulently and

10 deceitfully impersonated those institutions in order to induce Plaintiff and Class members to provide

11 their login credentials to Defendants, as described herein. Defendants did so without obtaining the

12 authority or approval of each financial institution.

13   196.   Plaintiff and Class members have been adversely affected by Defendants' violations

14 of the Anti-Phishing Act because Defendants engaged in this deceitful conduct in order to extract

15 from Plaintiff and Class members their login credentials and all of the transaction history and other

16 data accessible with those credentials, as detailed above. Defendants caused actual injury, harm,

17 damage and loss to Plaintiff and Class members for the reasons described herein.

18   197.   Plaintiff and Class members are entitled to relief under Cal. Bus. & Prof. Code

19 § 22948.3(a)(2), including $5,000 per violation, which damages should be trebled because

20 Defendants engaged in a pattern and practice of violating § 22948.2 (indeed, it is the essence of

21 Defendants' business model); an injunction against further violations; costs of suit and reasonable

22 attorney's fees; and such other relief as the Court may deem just and proper.

NINTH CAUSE OF ACTION

Violation of the Computer Fraud and Abuse Act
18 U.S.C. § 1030
(On Behalf of Plaintiff and the Classes)

26   198.   Plaintiff incorporates the substantive allegations contained in all prior and

27 succeeding paragraphs as if fully restated herein.

28

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

1

A.   VIOLATIONS OF 18 U.S.C. § 1030(A)(2)

2   199.   A person violates 18 U.S.C. § 1030(a)(2) if it "intentionally accesses a computer

3   without authorization or exceeds authorized access, and thereby obtains—(A) information contained

4   in a financial record of a financial institution . . . [or] (C) information from any protected computer."

5   Protected computers include computers "exclusively for the use of a financial institution . . . or . . .

6   used by . . . a financial institution . . . and the conduct constituting the offense affects that use by or

7   for the financial institution," 18 U.S.C. § 1030(e)(2)(A), or computers "used in or affecting interstate

8   or foreign commerce," 18 U.S.C. § 1030(e)(2)(B).

9   200.   The computer systems, data storage facilities, or communications facilities that

10 Plaintiff and Class members' financial institutions use to store Plaintiff and Class members' data

11 are "protected computers" under the statute because they are exclusively for the use of financial

12 institutions or, in the alternative, were affected by Defendants' conduct, or were used in or affected

13 interstate commerce. Defendants intentionally accessed these protected computers and thereby

14 obtained information contained in the financial institutions' financial records. Defendants did so

15 without authorization. To the extent that Defendants received any valid authorization, their conduct

16 exceeded that authorization for the reasons described above. *See* 18 U.S.C. 1030(e)(6) (defining the

17 term "exceeds authorized access" to mean "to access a computer with authorization and to use such

18 access to obtain or alter information in the computer that the accessor is not entitled so to obtain or

19 alter").

20

B.   VIOLATIONS OF 18 U.S.C. § 1030(A)(4)

21   201.   A person violates 18 U.S.C. § 1030(a)(4) if it "knowingly and with intent to defraud,

22 accesses a protected computer without authorization, or exceeds authorized access, and by means

23 of such conduct furthers the intended fraud and obtains anything of value, unless the object of the

24 fraud and the thing obtained consists only of the use of the computer and the value of such use is

25 not more than $5,000 in any 1-year period."

26   202.   Defendants knowingly accessed protected computers, and did so without

27 authorization or in excess of authorization, for the reasons described herein.

28   203.   Defendants acted with intent to defraud because they devised a scheme to deceive

1 Plaintiff and Class members into thinking that they were providing their banking credentials directly

2 to their bank, when in fact they were providing those credentials to Defendants. Through that

3 conduct, Defendants furthered their fraud and obtained things of value, namely, Plaintiff and Class

4 members' sensitive personal data.

5 **C.   VIOLATIONS OF 18 U.S.C. § 1030(A)(5)(A)**

6 204.   A person violates 18 U.S.C. § 1030(a)(5)(A) if it "knowingly causes the transmission

7 of a program, information, code, or command, and as a result of such conduct, intentionally causes

8 damage without authorization, to a protected computer."

9 205.   Defendants knowingly caused the transmission of a program, information, code or

10 command every time it sent Plaintiff's and Class members' credentials to their financial institutions.

11 Defendants did so without authorization for the reasons described herein. Defendants caused

12 damage for the reasons described herein.

13 **D.   VIOLATIONS OF 18 U.S.C. § 1030(A)(5)(B), (C)**

14 206.   A person violates 18 U.S.C. § 1030(a)(5)(B) if it "intentionally accesses a protected

15 computer without authorization, and as a result of such conduct, recklessly causes damage." A

16 person violates 18 U.S.C. § 1030(a)(5)(C) if it "intentionally accesses a protected computer without

17 authorization, and as a result of such conduct, causes damage and loss."

18 207.   Plaintiff's and Class members' financial institutions' computer systems, data storage

19 facilities, or communications facilities are protected computers under the statute for the reasons

20 described herein. Defendants acted without authorization for all of the reasons described herein.

21 Defendants acted not only recklessly but intentionally for all of the reasons herein. Defendants

22 caused damage or loss for the reasons described herein.

23 **E.   VIOLATIONS OF 18 U.S.C. § 1030(A)(6)**

24 208.   A person violates 18 U.S.C. § 1030(a)(6) if it "knowingly and with intent to defraud

25 traffics . . . in any password or similar information through which a computer may be accessed

26 without authorization, if—(A) such trafficking affects interstate or foreign commerce." The term

27 "traffic" means "transfer, or otherwise dispose of, to another, or obtain control of with intent to

28 transfer or dispose of." 18 U.S.C. § 1029(e)(5).

42

209.   Defendants acted knowingly and with intent to defraud for the reasons described herein. Defendants acted without authorization for the reasons described herein. Defendants trafficked in passwords and similar information when they obtained control of banking credentials from millions of distinct financial accounts with the intent of transferring them to their own massive database of user information, thus allowing Defendants access to Plaintiff's and Class members' financial institutions' computers. In the alternative, Defendants trafficked in passwords and similar information when, after acquiring Plaintiff's and Class members' login credentials under false pretenses and using them to login to those individuals' financial institutions, those institutions sent access tokens to Defendants, which access tokens Defendants then transferred to their app clients or partners.

210.   On information and belief, because of the locations of Defendants, their servers, and the millions of accounts for which Defendants acquired credentials and data, Defendants' trafficking activities affected interstate or foreign commerce.

II.   DEFENDANTS CAUSED ECONOMIC LOSS IN EXCESS OF $5,000, AS WELL AS OTHER DAMAGE

211.   Plaintiff may bring a private right of action for economic damages resulting from Defendants' violation of the CFAA, provided that Defendants 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).

212.   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, Defendants 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,

43

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.

213. Defendants' 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.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of herself and the proposed Class respectfully requests that the Court enter an order:

A. Certifying the Classes and appointing Plaintiff as Class Representative;

B. Finding that Defendants' conduct was unlawful as alleged herein;

C. Awarding declaratory relief against Defendants;

D. Awarding such injunctive and other equitable relief as the Court deems just and proper;

E. Awarding Plaintiff and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

F. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

G. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses, including expert costs; and

H. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Dated: August 25, 2020

/s/ Aaron M. Sheanin
Aaron M. Sheanin
Christine S. Yun Sauer
ROBINS KAPLAN LLP
2440 W El Camino Real, Suite 100
Mountain View, CA 94040
Telephone: (650) 784-4040
Facsimile: (650) 784-4041
asheanin@robinskaplan.com
cyunsauer@robinskaplan.com

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Hollis Salzman (*pro hac vice* forthcoming)
Kellie Lerner (*pro hac vice* forthcoming)
David Rochelson (*pro hac vice* forthcoming)
ROBINS KAPLAN LLP
399 Park Avenue, Suite 3600
New York, NY 10022
Telephone: (212) 980-7400
Facsimile: (212) 980-7499
hsalzman@robinskaplan.com
klerner@robinskaplan.com
drochelson@robinskaplan.com

Thomas J. Undlin (*pro hac vice* forthcoming)
ROBINS KAPLAN LLP
800 LaSalle Avenue, Suite 2800
Minneapolis, MN 55402
Telephone: (612) 349-8500
Facsimile: (612) 339-4181
tundlin@robinskaplan.com

Christian Levis (*pro hac vice* forthcoming)
Amanda Fiorilla (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com

Anthony M. Christina (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Telephone: (215) 399-4770
Facsimile: (914) 997-0035
achristina@lowey.com

Attorneys for Plaintiff and the Proposed Class

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL