Andrew N. Friedman (*pro hac vice*)
afriedman@cohenmilstein.com
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave. NW, Fifth Floor
Washington, DC 20005
Telephone: (202) 408-4600
Facsimile: (202) 408-4699

John A. Yanchunis (*pro hac vice*)
jyanchunis@ForThe People.com
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin St., 7th Floor
Tampa, FL 33602
Telephone: 813/223-5505
Facsimile: 813/223-5402

Ariana J. Tadler (*pro hac vice*)
atadler@Tadlerlaw.com
TADLER LAW LLP
One Penn Plaza
New York, New York
New York, NY 10119
Telephone: (212) 946-9453
Facsimile: (212) 273-4375
Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

STEPHEN ADKINS, an individual and Michigan resident, on behalf of himself and all others similarly situated,

Plaintiff,

v.

FACEBOOK, INC.,

Defendant.

No. C 18-05892 WHA (JSC)
Consolidated Cases:
No. C 18-06022 WHA (JSC)
No. C 19-00117 WHA (JSC)

AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

TABLE OF CONTENTS

INTRODUCTION

1. Facebook is a social networking site founded by Mark Zuckerberg. Over the decades, Facebook has amassed approximately 2.2 billion users.[1]

2. On September 28, 2018, Facebook disclosed that a breach of the company's network resulted in hackers obtaining direct access to the accounts of approximately 30 million Facebook users and all of the information accessible in and through those accounts (the "Data Breach")[2] The Data Breach was the result of software vulnerabilities that permitted access tokens—which enable people to stay logged into Facebook without reentering their password—to be taken.[3]

3. According to Facebook, the vulnerabilities permitting the Data Breach began in July 2017 and continued, undetected by Facebook, until September 2018.[4]

4. When Facebook initially discovered that hackers had exploited these vulnerabilities, it invalidated the access tokens of almost 90 million accounts that were potentially impacted.

5. Facebook ultimately conceded that 30 million users had their access tokens stolen.

6. Facebook further conceded that 29 million of those users had additional personally identifiable information ("PII") taken: For 15 million users, name and contact details (phone

---

[1] *Ad Targeting*, Facebook, Inc., https://www.facebook.com/business/products/ads/ad-targeting (last accessed Feb. 7, 2019).

[2] Brian Fung, *Facebook Says Millions of Users had Phone Numbers, Search History and Location Data Stolen in Recent Hack*, THE WASHINGTON POST (Oct. 12, 2018), *available at*: https://www.washingtonpost.com/technology/2018/10/12/facebook-says-fewer-users-were-affected-by-data-breach-more-information-was-taken/ (last accessed Oct. 24, 2018). Facebook originally reported that 50 million accounts were affected by the Data Breach, but later revised that number to 30 million. Plaintiff reserves the right to pursue relief for all Facebook users affected by the "View As" vulnerabilities revealed in discovery.

[3] *Id.*

[4] Guy Rosen, *An Update on the Security Issue*, Facebook Newsroom (Oct. 12, 2018), https://newsroom.fb.com/news/2018/10/update-security-issue/ (last accessed Jan. 29, 2019).

number, email, or both, depending on what people had on their profiles) were accessed. For 14 million users, the attackers accessed the same two sets of information (name and contact details), as well as username, gender, locale/language, relationship status, religion, hometown, self-reported current city, birthdate, device types used to access Facebook, education, work history, the last 10 places they checked into or were tagged in, website, people or pages they follow, and their 15 most recent searches.[5] Facebook has acknowledged a third set of users were affected by the Data Breach, but has not provided details of what was breached beyond users' tokens.[6]

7. The stolen PII has great value to criminals, researchers, advertisers, and political campaigns.

8. Specifically, experts say that these personal details "can be just as important to consumers—and valuable to criminals—as financial data."[7] In fact, such details may be more valuable than a Social Security Number or credit card information. Justin Brookman, director of privacy and technology policy for Consumers Union, the policy and mobilization division of Consumer Reports, said of the Data Breach, "Most data breaches involve financial information, but your Facebook account can be misused in a number of ways that are harmful. Accessing your private communications and posts by itself is pretty invasive, but that information could also be used to crack account security questions or to scam you and your friends."[8]

9. The PII certainly has great value to Facebook.

10. While Facebook offers a free social networking service, its ability to monetize the data of its users garner it great wealth.

---

[5] *Id.*
[6] *Id.*
[7] Allen St. John, *Facebook Breach Exposed Personal Data of Millions of Users: Hackers could find out your birthplace, religion, gender, and relationships. What you can do about it*, CONSUMER REPORTS (Oct. 12, 2018), https://www.consumerreports.org/digital-security/facebook-data-breach-exposed-personal-data-of-millions-of-users/ (last accessed Oct. 22, 2018).
[8] *Id.*

11. In 2018, Facebook's annual revenue was nearly $56 billion.[9] In 2017, Facebook's annual revenue was $40.65 billion, and the clear majority of Facebook's revenue—approximately 96%—originated from the sale of targeted advertising based on the extensive data Facebook collects, analyzes, and maintains about its users.[10] Facebook users effectively make a deal with Facebook: in exchange for their data (that Facebook monetizes), Facebook will honor privacy settings and protect that data from others. Plaintiff and users then share PII in their profiles or on Facebook messenger, creating a fiduciary relationship between Facebook and its users.

12. Facebook had previously agreed to a 2011 Federal Trade Commission Consent Order to better protect user privacy and prevent third parties from misappropriating personal information.

13. Plaintiff brings these actions on behalf of all persons who registered for Facebook in the United States and whose PII was compromised in the Data Breach as a result of Facebook's failure to: (i) adequately protect its users' PII, (ii) warn users of its inadequate information security practices, and (iii) effectively monitor and control those on Facebook's network that present a threat. Facebook's conduct amounts to negligence.

14. Plaintiff and similarly situated Facebook users ("Class members") have suffered injury as a result of Facebook's conduct. These injuries may include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, at an the estimated average loss of $18.70 per hour in lost labor hours,[11] (iv) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of

---

[9] Martina Frascona Sochurkova, *Facebook's Revenue Exceeded $55 Billion in 2018.* Newsfeed.org (July 2, 2019), available at: https://newsfeed.org/facebooks-revenue-exceeded-55-billion-in-2018/

[10] Annual Reports, Facebook, Inc., (2012, 2014, 2017); 10-K Quarterly Reports, Facebook, Inc., (Q2 2018).

[11] Plaintiff's March 7, 2019 Amended Initial Disclosures pursuant to Rule 26(a) at p. 23-24.

customers and former customers in their continued possession; and (v) future costs in terms of loss of time, effort, and money that will be expended to monitor, prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members.

15. Finally, because Facebook knew for years about the security vulnerability that led to the Data Breach and consciously disregarded the risk it posed to the safety of users' PII, punitive damages are also appropriate.

PARTIES

16. Plaintiff Stephen Adkins is a citizen and resident of Michigan, and over the age of eighteen years. Plaintiff Adkins has had a Facebook account since March 4, 2009.

17. Defendant Facebook, Inc. ("Facebook"), is incorporated in Delaware, and its principal place of business is 1601 Willow Road, Menlo Park, CA 94025; it is thus a citizen of Delaware and California.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant. Moreover, Plaintiff Stephen Adkins is a citizen of Michigan and therefore diverse from Facebook, which is headquartered in California and incorporated in Delaware.

19. This Court has personal jurisdiction over Defendant because Facebook is headquartered in California and conducts business in the state of California.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Venue is also proper because Facebook's terms of service require that claims are resolved "exclusively in the U.S. District Court for the Northern District of California or a state

court located in San Mateo County . . ."[12]

FACTUAL ALLEGATIONS

A. Users Provide Valuable PII in Exchange for Facebook's Service

21. Users must provide Facebook with PII to use Facebook's service.

22. PII is valuable currency to the users because they can exchange it for services from internet companies like Facebook. A recent article estimates that users would have to pay $10 per month in exchange for an ad-free version of Facebook that does not rely on collecting users' PII.[13]

23. Likewise, PII is valuable to Facebook, because Facebook depends on users' PII for advertising revenue. For instance, Facebook's acquisitions of Instagram and WhatsApp indicate that Facebook, at a minimum, put a value of $33 or $42 for each class member's PII. In April 2012, Facebook acquired Instagram (a photo sharing app) for $1 billion, paying the equivalent of $33 per Instagram user. In February 2014, Facebook paid approximately $19 billion for WhatsApp (a smartphone app that allow you to send text messages, photos and videos) or $42 per user.

24. A market exists for stolen PII because malicious actors are able to monetize that information by gaining access to both metadata attached to the PII and by harvesting valuable information from the users' accounts themselves. An individual's entire portfolio of PII has been valued as high as $1,200 per person.[14] Based solely on the type of PII that Facebook has publicly asserted was taken in the Data Breach, the value of that information on the Dark Web ranges from $15 to $30 per person.[15]

25. In exchange for their PII, Plaintiff and Class members received a benefit equivalent

---

[12] *Terms of Service*, Facebook, Inc., https://www.facebook.com/terms.php (last accessed July 8, 2019). The Terms of Service for "Disputes" also state that "the laws of California will govern these Terms and any claim, without regard to conflict of law provisions."

[13] Rani Molla, *The Cost of an Ad-Free Internet: $35 More Per Month*, Vox.com (Jun. 24, 2019) https://www.vox.com/recode/2019/6/24/18715421/internet-free-data-ads-cost.

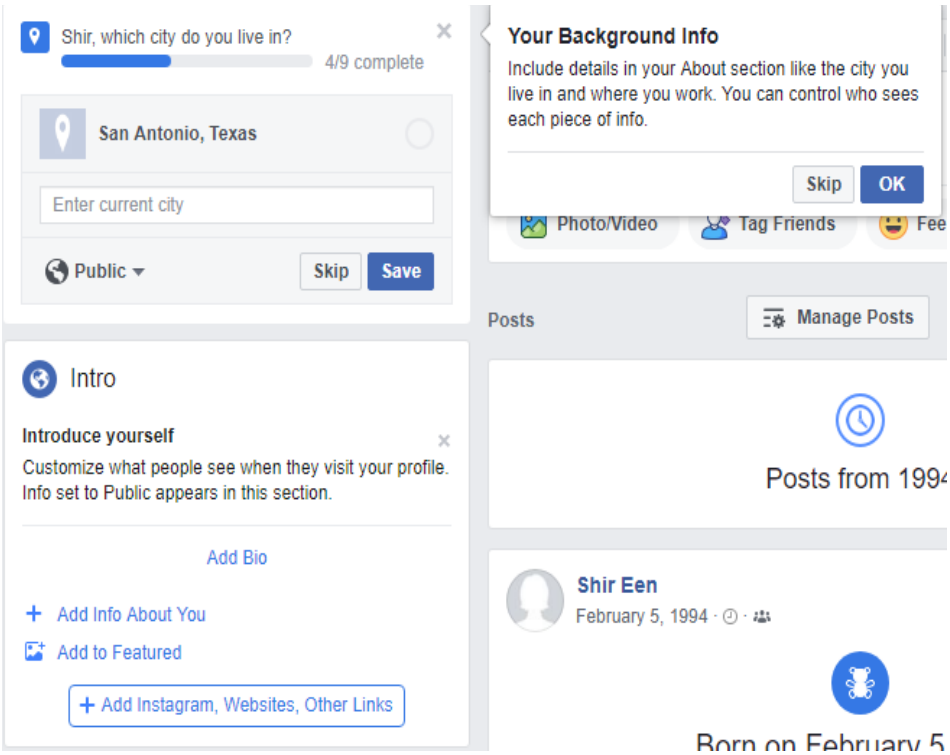
[14] Migliano, Simon, *Dark Web Market Price Index (US Edition)*, top10VPN.com (Feb. 27, 2018). https://www.top10vpn.com/news/privacy/dark-web-market-price-index-feb-2018-us/

[15] Plaintiff's March 7, 2019 Amended Initial Disclosures pursuant to Rule 26(a) at p. 21.

to the value of Facebook's service. Plaintiff and Class members clearly intended to and did participate in the online information exchange market in which PII functions as money paid for the use of social media platforms and the like. Due to Facebook's misconduct and the resulting Data Breach, hackers obtained that PII at no compensation to Plaintiff and Class members whatsoever.

B. The Facebook Profile

26. When a person opens a Facebook account, he or she is prompted to include certain information on his or her profile page.



27. To create an account, a person is required to share his/her name, email address or mobile phone number, date of birth, and gender.

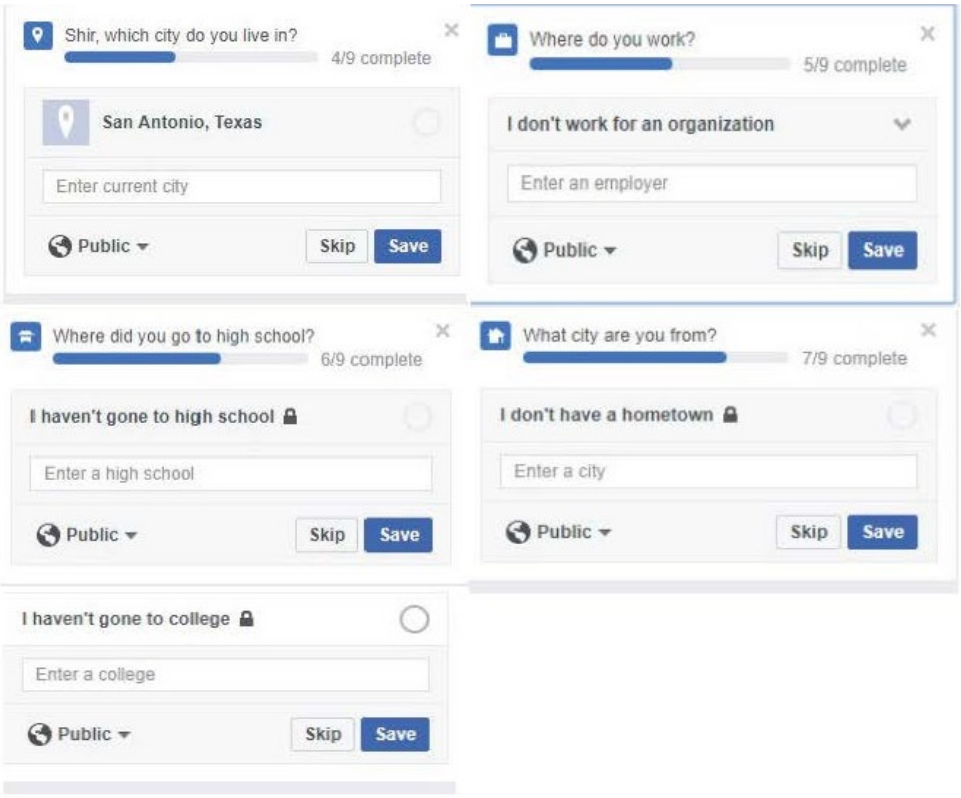
28. Most of the other requested information can be called historical PII, such as hometown, employment, and educational history.

29. This information helps Facebook connect those viewing the site with "friends," and increase its user base.

30. To reset the account or apply Facebook-recommended security controls, a Facebook

user must supply a copy of their complete driver's license and a second mobile phone number.

31. The "privacy" settings for this PII defaults to "public" unless the user toggles it to a higher privacy setting. Below, pictured together (instead of single screen shots) are some of the screens a user would see:



32. The user will also receive prompts from Facebook to "update info" and to add this additional PII, as well as email addresses and phone numbers, to his or her profile page.

C. Facebook's Terms of Service, Data Policy and Privacy Principles

33. There is not one integrated contract that spells out Facebook's obligations to the user, but those obligations can be determined by reference to Facebook's course of dealing with the Class, industry practice, and from various webpages created by Facebook, including Facebook's "Terms of Service" section (https://www.facebook.com/terms.php); "How You're Protected" section (https://www.facebook.com/about/basics/stay-safe-and-secure/how-youre-protected); Facebook's "Privacy Principles" (https://www.facebook.com/about/basics/privacy-

principles), and Facebook's "Data Use Policy" (https://www.facebook.com/full_data_use_policy).

i. Terms of Service – the Basics

34. When a user opens a Facebook account, he or she must agree to a "Terms of Service" ("Terms").[16] These Terms create mutual obligations for Facebook and its users.

35. The Terms set out what services Facebook provides ("Our Services"), stating, in part:

a. "… a personalized experience for you …"

b. "Connect you with people and organizations you care about …"

c. "Help you discover content, products, and services that may interest you …"

d. "Combat harmful conduct and protect and support our community…"

e. "Enable global access to our services; to operate our global services, we need to store and distribute content and data in our data centers and systems around the world, including outside your country of residence."[17]

36. The Terms set out "Commitments" or obligations of the Facebook user, including that the user provides the same name used in everyday life, provide accurate information, and "Not share their password or give access to their Facebook account to others." (the "Commitments").[18]

37. The Commitments require that the user adhere to "Community Standards" and the Terms, not engage in fraud or upload viruses or malicious codes, and "not access or collect data from our Products using automated means (without our prior permission) or attempt to access data you do not have permission to access."

38. Facebook explains that the user provides his or her data and content in consideration for his or her social networking experience.

39. For example, the Terms set out that the user gives Facebook permission to use

---

[16] *Terms of Service*, Facebook, Inc., https://www.facebook.com/terms.php (last accessed Feb. 7, 2019).

[17] *Id.*

[18] *Id.*

content that the user creates and shares, and to share information about the user's action with ads and sponsored content.[19]

40. Finally, the Terms state that the laws of California govern the Terms and any claims and designate the Northern District of California as the venue for any for any dispute.[20]

ii. Data Policy

41. On the "Terms of Service" webpage, under item "5. Other terms and policies that may apply to you," is a link to Facebook's Data Policy. It states in part:

> 2. Our Data Policy and Your Privacy Choices
> To provide these services, we must collect and use your personal data. We detail our practices in the Data Policy, which you must agree to in order to use our Products.
> We also encourage you to review the privacy choices you have in your settings.

42. The Data Policy further informs:

> How do we operate and transfer data as part of our global services?
> We share information globally, both internally within the Facebook Companies, and externally with our partners and with those you connect and share with around the world in accordance with this policy. Your information may, for example, be transferred or transmitted to, or stored and processed in the United States or other countries outside of where you live for the purposes as described in this policy. These data transfers are necessary to provide the services set forth in the Facebook Terms and Instagram Terms and to globally operate and provide our Products to you. *We utilize standard contract clauses*, rely on the European Commission's adequacy decisions about certain countries, as applicable, and obtain your consent for these data transfers to the United States and other countries.[21] (emphasis added).

43. If one clicks on the hyperlink for "standard contract clauses", they are taken to the following URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087. This February 5, 2010 European Commission decision regarding data protection sets out certain obligations regarding data protection. For example:

> (12) Standard contractual clauses should provide for the technical and

---

[19] *Id.*
[20] *Id.*
[21] https://www.facebook.com/full_data_use_policy

organisational security measures to be applied by data processors established in a third country not providing adequate protection, in order to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. Parties should make provision in the contract for those technical and organisational measures which, having regard to applicable data protection law, the state of the art and the cost of their implementation, are necessary in order to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access or any other unlawful forms of processing.

The Data Policy further states:

a. **Information and content you provide**. We collect the content, communications and other information you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others. This can include information in or about the content you provide (like metadata), such as the location of a photo or the date a file was created. It can also include what you see through features we provide, such as our camera . . . Our systems automatically process content and communications you and others provide to analyze context and what's in them . . .

b. **Network and connections**. We collect information about the people, Pages, accounts, hashtags and groups you are connected to and how you interact with them across our Products, such as people you communicate with the most or groups you are part of. We also collect contact information if you choose to upload, sync or import it from a device (such as an address book or call log or SMS log history) . . .

c. **Your usage**. We collect information about how you use our Products, such as the types of content you view or engage with; the features you use; the actions you take; the people or accounts you interact with; and the time, frequency and duration of your activities. For example, we log when you're using and have last used our Products, and what posts, videos and other content you view on our Products. We also collect information about how you use features like our camera.

d. **Information about transactions made on our products.** If you use our Products for purchases or other financial transactions (such as when you make a purchase in a game or make a donation), we collect information about the purchase or transaction. This includes payment information, such as your credit or debit card number and other card information; other account and authentication information; and billing, shipping and contact details.

e. **Things others do and information they provide about you.** We

> also receive and analyze content, communications and information that other people provide when they use our Products. This can include information about you, such as when others share or comment on a photo of you, send a message to you, or upload, sync or import your contact information.
>
> f. We collect information from and about the computers, phones, connected TVs and other web-connected devices you use that integrate with our Products, and we combine this information across different devices you use. For example, we use information collected about your use of our Products on your phone to better personalize the content (including ads) or features you see when you use our Products on another device, such as your laptop or tablet, or to measure whether you took an action in response to an ad we showed you on your phone on a different device.
>
> g. Advertisers, app developers, and publishers can send us information through Facebook Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about your activities off Facebook—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services—whether or not you have a Facebook account or are logged into Facebook. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its store. We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information.[22]

44. In its section entitled "Sharing with Third-Party Partners," Facebook explains that, while it does not sell any of the user's information to third parties, it does provide advertisers with reports about the kinds of people seeing their ads and information about users to measurement partners and facilitates payments with vendors who sell to users on Facebook.

45. Facebook justifies this use by noting this sharing "makes it possible to operate our companies and provide free service to people around the world."[23]

---

[22] *Data Policy*, Facebook, Inc., https://www.facebook.com/about/privacy (last accessed Feb. 7, 2019).
[23] *Id.*

46. Facebook actively solicits as much information as possible from its users and monetizes that information.[24]

47. In addition, some users' accounts also contain payment card information, and Facebook has actively encouraged banks to join its Messenger app and bring "users' financial information, like credit card transactions and checking account balances" along with them.[25]

48. Facebook acknowledges that with the information it holds comes a responsibility to protect it. Facebook specifically promises that "[w]hen it comes to your personal information, we don't share it without your permission (unless required by law)."[26]

49. Facebook's Data Policy further represents that Facebook "[p]romotes safety, integrity, and security" by "us[ing] the information we have to verify accounts and activity, combat harmful conduct, detect and prevent spam and other bad experiences, maintain the integrity of our Products, and promote safety and security on and off of Facebook Products."

50. Facebook's Data Use Policy, updated in January 2015, also provides, in relevant part:

> Granting us permission to use your information not only allows us to provide Facebook as it exists today, but it also allows us to provide you with innovative features and services we develop in the future that use the information we receive about you in new ways. While you are allowing use to use the information we receive about you, you always own all of your information. Your trust is important to us, which is why we don't share information we receive about you with others unless we have:
>
> - received your permission
> - given you notice, such as by telling you about it in this policy; or
> - removed your name and any other personally identifying

---

[24] John Constine, *Facebook's Revenue Growth Strategy: Ad Targeting by In-App Behavior*, TECHCRUNCH (Feb. 1, 2012), *available at*: https://techcrunch.com/2012/02/01/action-spec-ad-targeting.

[25] Sara Salinas, *Facebook is asking more financial institutions to join Messenger*, CNBC (Aug. 6, 2018), *available at*: https://www.cnbc.com/2018/08/06/facebook-messenger-could-soon-feature-your-bank-information.html.

[26] *Privacy Basics*, Facebook, Inc., https://www.facebook.com/about/basics/stay-safe-and-secure/how-youre-protected (last accessed Feb. 7, 2019).

information from it.[27]

iii. Privacy Principles

51. From the Facebook "Terms of Service" page (https://www.facebook.com/terms.php.), one could also find the link for "Privacy Basics" (https://www.facebook.com/about/basics). Within those pages are Facebook's "Privacy Principles" (https://www.facebook.com/about/basics/privacy-principles). Those state, in relevant part, that:

> **We design privacy into our products from the outset**
> We design privacy into Facebook products with guidance from experts in areas like data protection and privacy law, security, interface design, engineering, product management, and public policy. Our privacy team works to build these diverse perspectives into every stage of product development.
>
> **We work hard to keep your information secure**
> We work around the block to help protect people's accounts, and we build security into every Facebook product. Our security systems run millions of time per second to help catch threats automatically and remove them before they ever reach you . . .
>
> **You own and can delete your information**
> You own the information you share on Facebook. This means you decide what you share and who you share it with on Facebook, and you can change your mind . . .
>
> **Improvement is constant**
> We're constantly working to develop new controls and design them in ways that explain things to people clearly. We invest in research and work with experts beyond Facebook including designers, developers, privacy professionals and regulators.
>
> **We are accountable**
> In addition to comprehensive privacy reviews, we put products through rigorous security testing. We also meet with regulators, legislators and privacy experts around the world to get input on our data practices and

[27] *2015 Data Policy*, Facebook, Inc., https://web.archive.org/web/20141223083330/https://www.facebook.com/full_data_use_policy (last accessed Feb. 7, 2019).

policies.[28]

D. Facebook Has Been on Notice of Privacy Issues and Misuse of Its Data But Has Repeatedly Failed to Prevent Data Incursions

52. Facebook has a long history of misleading users about the adequacy of its data protection.

53. Facebook's founder Mark Zuckerberg infamously stated that Facebook's motto was "Move fast and break things," often plastered across Facebook's campus as a reminder that non-conformist hackers were running the social network company.[29] That motto was axed in 2014, when Mr. Zuckerberg shifted the motto to "Move fast with stable infrastructure."[30]

54. However, in November 2007, Facebook faced backlash from its then-57 million users for its privacy abuses with the now-defunct "Beacon" feature.[31] Zuckerberg admitted that Facebook and its team of engineers "made a lot of mistakes building [Beacon], but we've made even more with how we've handled them. We simply did a bad job with this release, and I apologize for it."[32] The apology came after a groundswell of users complaining that Facebook deceived its users and tracked far more information with Beacon than originally represented, prompting a petition with MoveOn.org and a $9.5 million class action settlement concerning Facebook's privacy practices.[33]

55. In July 2008, a "glitch" in Facebook's code exposed the birthdates of approximately

---

[28] *Id.*

[29] Nick Statt, *Zuckerberg: 'Move Fast and Break Things' isn't how Facebook Operates Anymore*, C|NET (April 30, 2014), *available at*: https://www.cnet.com/news/zuckerberg-move-fast-and-break-things-isnt-how-we-operate-anymore/

[30] *Id.*

[31] Andrew Clark, *Facebook Apologies for Mistakes over Advertising*, THE GUARDIAN (Dec. 6, 2007), *available at*: https://www.theguardian.com/technology/2007/dec/06/facebook.socialnetworking.

[32] *Id.*

[33] David Kravets, *Facebook's $9.5 Million "Beacon" Settlement Approved*, WIRED (Sept. 21, 2012), *available at* https://www.wired.com/2012/09/beacon-settlement-approved/

80 million users.[34]

56. Facebook did not identify the "glitch" internally; rather, a third-party technology consultant discovered the "glitch" when he was reviewing Facebook's new design and noticed that the birthdates "of his privacy-obsessed acquaintances were popping up when they should have been hidden."[35]

57. Although Facebook purportedly allowed users to control the audience of users who could see aspects of a user's profile, Facebook's new design made the information public to other Facebook users, essentially ignoring the users' privacy settings.[36]

58. At the time, Facebook could not determine how long the data was exposed, or identify how many people viewed the data, because even though the new design was in beta form and supposed to be shielded from public access, non-beta-tester users still had access.[37]

59. In 2011, Facebook settled with the Federal Trade Commission over charges it had deceived users by "telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public."[38] Facebook agreed to make its privacy and data sharing policies more prominent and was "barred from making misrepresentations about the privacy or security of consumers' personal information" while also being "required to establish and maintain a comprehensive privacy program designed to address privacy risks associated with the development and management of new and existing products and services, and to protect the privacy

---

[34] Robert McMillan, *Facebook Bug Leaks Members' Birthday Data*, CSO ONLINE (July 17, 2008), *available at*: https://www.csoonline.com/article/2123018/identity-theft-prevention/facebook-bug-leaks-members--birthday-data.html.

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] *Facebook Settles FTC Charges that it Deceived Consumers by Failing to Keep Privacy Promises*, THE UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION (Nov. 29, 2011), *available at*: https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep

and confidentiality and consumers' information."[39] This program was specifically required to be "appropriate to [Facebook's] size and complexity, the nature and scope of [Facebook's] activities, and the sensitivity of the covered information, including . . . . the identification of reasonably foreseeable, material risks, both internal and external, that could result in . . . disclosure of covered information . . ."[40]

60. Around the same time, following a legal complaint by a European privacy campaigner, Facebook was urged by the Irish Data Protection Commissioner to tighten up app permissions to avoid "friends" data leakage. However, Facebook did not tighten permissions until 2015.[41]

61. In 2013, Facebook exposed six million users' contact information (email addresses and phone numbers) to unauthorized third parties.[42] Like with prior privacy violations and the violations at issue in this litigation, the vulnerability existed for at least five months before a third party identified the vulnerability and brought it to Facebook's attention.[43]

62. Not only did the vulnerability permit unauthorized access to those six million users' contact information, it also permitted unauthorized third parties access to non-users' contact information—that is, contact information Facebook collected related to individuals who never

---

[39] *Id.*

[40] Order Containing Consent Order, *In the Matter of Facebook, Inc.*, File No. 092 3184, THE UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION, *available at*: https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf

[41] Natasha Lomas, *Facebook Data Misuse Scandal Affects 'Substantially' More than 50M, Claims Wylie*, TECHCRUNCH (March 27, 2018), *available at*: https://techcrunch.com/2018/03/27/facebook-data-misuse-scandal-affects-substantially-more-than-50m-claims-wylie

[42] Billy Gallagher, *Facebook Security Bug Exposed Personal Account Information, Emails and Phone Numbers, Six Million Accounts Affected*, TECHCRUNCH (June 21, 2013), *available at*: https://techcrunch.com/2013/06/21/facebook-security-bug-exposed-personal-account-information-emails-and-phone-numbers-six-million-accounts-affected/

[43] Alexis Kleinman, *Facebook Bug Exposed Email Addresses, Phone Numbers of 6 Million Users*, THE HUFFINGTON POST (June 21, 2013), *available at*: https://www.huffingtonpost.com/2013/06/21/facebook-bug_n_3480739.html

signed up for, logged into, or used the Facebook platform.[44]

63. In 2015, Facebook detected that political firm Cambridge Analytica was misusing personal data to create, among other things, targeted political ads. Its lawyers sent a letter to Cambridge Analytica in August of 2016 asking for verification that any such data be deleted. Facebook accepted a letter from Cambridge Analytica that it had done so but did not bother to follow up or conduct a forensic audit.[45]

64. When identifying Cambridge Analytica as the entity that misappropriated Facebook data, Facebook founder and CEO Mark Zuckerberg admitted Facebook's negligence in the scandal: "But it's clear now that we didn't do enough to prevent [our] tools from being used for harm as well. That goes for the fake news, foreign interference in elections, and hate speech, as well as developers and *data privacy*. We didn't take a broad enough view of our responsibility, and that was a big mistake." (Emphasis added.)

65. Zuckerberg made further admissions regarding Facebook's failure to protect the PII of its users:

> We have a responsibility to protect your data, and if we can't then we don't deserve to serve you. I've been working to understand exactly what happened and how to make sure this doesn't happen again.[46]
>
> I'm sorry we didn't do more at the time. We're now taking steps to ensure this doesn't happen again.[47]

66. When called to testify before a joint session of the Senate Commerce Committee and

---

[44] Gallagher, *supra* n.48.
[45] Natasha Lomas, *Facebook Data Misuse Scandal Affects 'Substantially' More than 50M, Claims Wylie*, TECHCRUNCH (March 27, 2018), *available at*: https://techcrunch.com/2018/03/27/facebook-data-misuse-scandal-affects-substantially-more-than-50m-claims-wylie
[46] Sam Meredith, *Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal*, CNBC (Apr. 10, 2018), *available at*: https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html
[47] *Id.*

Judiciary Committee, in April 2018, Zuckerberg was chastened by many congresspeople, including Senator Bill Nelson of Florida, who said, "Let me just cut to the chase. If you and other social media companies do not get your act in order, none of us are going to have privacy anymore . . . We're talking about personally identifiable information that, if not kept by the social media . . . companies from theft, a value that we have in America, being our personal privacy – we won't have it anymore."[48]

67. Zuckerberg admitted that "we need to now take a more active view in policing the ecosystem" and that, "at the end of the day, this is going to be something where people will measure us by our results . . ."[49]

68. Zuckerberg was specifically questioned by Senator Tammy Baldwin of Wisconsin regarding whether "Facebook [could] be vulnerable to a data breach or hack . . ." He answered, "there are many kinds of security threats that a company like ours faces, including people trying to break in to our security systems" and stated that if Facebook was hacked, he believed that he would have the duty to inform those impacted.[50]

69. In a recognition of culpability, Zuckerberg further told the Joint Committees:

> We didn't take a broad enough view of our responsibility, and that was a big mistake. And it was my mistake. And I am sorry. I started Facebook, I run it, and I'm responsible for what happens here.
>
> So, now, we have to go through our — all of our relationship with people and make sure that we're taking a broad enough view of our responsibility. It's not enough to just connect people. We have to make sure that those connections are positive. It's not enough to just give people a voice. We need to make sure that people aren't using it to harm other people or to spread misinformation. And it's not enough to just give people control over their information. We need to make sure that the developers they share it with protect their information, too. Across the

---

[48] *Transcript of Mark Zuckerberg's Senate Hearing*, THE WASHINGTON POST (Apr. 10, 2018), *available at*: https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?noredirect=on&utm_term=.c7f29f9a3e4d

[49] *Id.*

[50] *Id.*

> board, we have a responsibility to not just build tools, but to make sure that they're used for good.[51]

70. Zuckerberg stated plainly in response to a question from Senator Cantwell, "Senator, I think everyone in the world deserves good privacy protection." Facebook committed to "putting stronger protections in place to prevent future abuse of our platform."[52]

71. However, as recently as January 2019, Facebook has again been under fire for its disregard for both user privacy and developer protocols.

72. Apple banned Facebook from offering apps and updates on Apple's platform after discovering that Facebook had "violat[ed] Apple's rules with a research app that allowed Facebook to snoop on users' online activity."

73. The app at issue was reportedly part of a Facebook program known as Project Atlas which paid users $20 to install an app on their Apple devices called "Facebook Research." The app was offered to minors as well as adults and permitted Facebook "to track app use, the websites visited, the Amazon purchases they made and other intimate data."

74. The app also circumvented Apple's usual download process through the App Store and was uploaded through a process that trusted web developers are only permitted to use for internal testing under their agreements with Apple.[53]

75. By late May 2019, Facebook's own lawyers took the position that users could not have any expectation of privacy on Facebook.[54]

76. A longtime consultant to Facebook and former mentor to Mark Zuckerberg, Roger

---

[51] *Id.*

[52] *How is Facebook Working to Keep its Community Safe?*, Facebook, Inc., available at: https://www.facebook.com/help/208040513126776?helpref=popular_topics (last accessed Feb. 7, 2019).

[53] Kevin Roose, *Maybe Only Tim Cook Can Fix Facebook's Privacy Problem*, THE NEW YORK TIMES (Jan. 30, 2019), *available at*: https://www.nytimes.com/2019/01/30/technology/facebook-privacy-apple-time-cook.html.

[54] Hannah Albazari, *Facebook Says Social Media Users Can't Expect Privacy*, LAW360 (May 29, 2019), *available at:* https://www.law360.com/articles/1164091

McNamee, wrote an op-ed in TIME magazine in January lamenting what has happened to Facebook, and how it developed to something which brought him shame:

> To feed its AI and algorithms, Facebook gathered data anywhere it could. Before long, Facebook was spying on everyone, including people who do not use Facebook. Unfortunately for users, Facebook failed to safeguard that data. Facebook sometimes traded the data to get better business deals. These things increased user count and time on-site, but it took another innovation to make Facebook's advertising business a giant success.
>
> From late 2012 to 2017, Facebook perfected a new idea-growth hacking-where it experimented constantly with algorithms, new data types and small changes in design, measuring everything. Growth hacking enabled Facebook to monetize its oceans of data so effectively that growth-hacking metrics blocked out all other considerations. In the world of growth hacking, users are a metric, not people.[55]

77. On July 12, 2019, the FTC voted to fine Facebook a record-setting $5 billion for mishandling users' personal information.[56]

E. Facebook's Privacy Features Result in Unwanted Disclosures

78. As noted by McNamee, Facebook's primary revenue model relies on users to share as much PII as possible with as few hurdles and limitations for sharing that PII on the Facebook platform as possible. To maximize revenue, Facebook has not always honored the privacy settings of its users.

79. Many users depend on user-to-user privacy within the Facebook platform (i.e., only sharing posts with friends or certain subgroups of friends).

80. Nevertheless, Facebook violated its own policy in October 2015 when it updated its search engine, at the expense of users' privacy, without alerting users.[57]

---

[55] Roger McNamee, *I Mentored Mark Zuckerberg. I Loved Facebook. But I Can't Stay Silent About What's Happening*, TIME (Jan. 17. 2019), *available at*: http://time.com/5505441/mark-zuckerberg-mentor-facebook-downfall/.

[56] Cecilia Kang, *FTC Approves Facebook Fine of About $5 Billion*, THE NEW YORK TIMES (July 12, 2019) available at: https://www.nytimes.com/2019/07/12/technology/facebook-ftc-fine.html

[57] Alex Hern, *Facebook is Chipping away at Privacy – and my Profile has been Exposed*, THE

81. Facebook's new internal search engine made searching within the Facebook platform easier but, in the process, all private profiles were publicly searchable—even for non-users and on platforms outside of Facebook, such as Google's or Yahoo's search engines.[58]

82. Although users' privacy settings permitted them to set their profiles so that only certain users could see their profiles and information contained therein, the updated search function switched these profiles to public.[59]

83. Without the benefit of an "opt out" option, users' posts, photos, and other activity not specifically set to the most private setting (a setting the user would have to manually check for each post, photo, and other activity) were now exposed beyond the Facebook platform, despite users having limited their privacy settings to prevent such disclosure of their personal information.[60]

84. This meant those posts—previously limited to a small group of people—were now completely visible and searchable and, worse, Facebook's new search feature would scan the user's profile and use that information to autocomplete another user's search.[61]

85. For example, if hypothetical user Sally Smith "liked" the band "Tom Petty & the Heartbreakers" in her private profile, and another user (not necessarily her friend) searched for "Sally Smith Tom Pe," Facebook's new search feature would autocomplete the search to "Sally Smith Tom Petty & the Heartbreakers," thus revealing Sally Smith's otherwise and believed-to-be private information.

86. Users may "like" or "post" items related to several particularly sensitive topics, e.g., health issues, religion, politics, familial issues.

87. These examples are not limited to individual users' searches; game developers,

---

GUARDIAN (June 29, 2016), *available at*: https://www.theguardian.com/technology/2016/jun/29/facebook-privacy-secret-profile-exposed.

[58] *Id.*

[59] *Id.*

[60] *Id.*

[61] *Id.*

application developers, marketers, and other third-party vendors had access to this search function and could use it to exploit information that users otherwise believed to be private.[62]

F. Despite Repeated Assurances to the Public and its Users, Facebook Suffered Another Preventable Data Breach.

88. When a user logged into Facebook with his or her username and password, Facebook then generated an access token for that user. This access token operated as an automatic super password—an all-purpose key that mapped to a user's profile—which allowed a user to log in numerous times without typing out their username and password each time. This practice streamlined logins and reduced the barriers for users to access the Facebook platform and provide PII.

89. Industry-standard information and data security best practices demand that companies that utilize access tokens should limit the lifespan of those access tokens to a reasonable period (e.g., an hour, a day, a week, a month).

90. Once Facebook provided a user with an access token, however, Facebook did not subsequently expire the access token—the access tokens remained valid for months or even years. Facebook never required the user subsequently to provide her or his username and password (e.g., an hour, a day, a week, or a month later) to reissue the access token. The access token remained valid for an indefinite period.

91. According to Facebook, it first became aware of a potential data breach on September 14, 2018, when it noticed "an unusual spike of activity."[63]

92. Facebook allowed the attackers to gain access to over 400,000 Facebook accounts, and steal 30 million Facebook users' "access tokens," which are "the equivalent of digital keys."[64]

---

[62] Amy X. Wang, *How to Keep Facebook's Powerful new Search Engine from Unearthing your Old, Embarrassing Posts*, QUARTZ (Oct. 22, 2015), *available at*: https://qz.com/531244/how-to-keep-facebooks-powerful-new-search-engine-from-unearthing-your-old-embarrassing-posts/.
[63] Allen St. John, *supra* n.7.
[64] Guy Rosen, *supra* n.4.

93. With access to users' tokens, the attackers siphoned purportedly 29 million users' PII without any form of intervention, interruption, or difficulty until September 25, 2018, when Facebook allegedly first determined the increased network traffic was actually an attack.[65]

94. On September 25, 2018, 11 days after the attack allegedly began, Facebook's engineering team discovered the security issues that resulted in the Data Breach.

95. Three separate vulnerabilities in Facebook's code had permitted unauthorized individuals to utilize Facebook's "View As" feature—which permits users to see what their profile looks like to others—to steal access tokens (which are designed to enable users to stay logged into Facebook without reentering their password).[66]

96. With these access tokens, the unauthorized individuals were able to take over users' accounts.[67]

97. Access tokens are used by Facebook to authenticate users. Facebook describes them as "the equivalent of digital keys that keep people logged in to Facebook so they don't need to re-enter their password every time they use the app."[68]

98. Ironically, two of the software vulnerabilities were the result of Facebook introducing an online tool to *improve* privacy for users, while the third was introduced to ease the uploading of birthday videos. Once Facebook discovered the Data Breach, it claims it "invalidated the access tokens of almost 90 million accounts that were potentially impacted by the vulnerability" while it investigated the breach. This resulted in a forced logout of these users, requiring them to reenter their passwords.[69]

---

[65] *Id. See also* "Facebook' Statement", ECF No. 61 at 5.
[66] Mike Isaac & Sheera Frenkel, *Facebook Security Breach Exposes Accounts of 50 Million Users*, THE NEW YORK TIMES (Sept. 28, 2018), *available at*: https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html.
[67] *Security Update*, Facebook, Inc., *available at*: https://newsroom.fb.com/news/2018/09/security-update/ (last accessed Feb. 7, 2019).
[68] *Id*.
[69] *An Important Update about Facebook's Recent Security Incident*, Facebook, Inc., *available at*:

99. Beginning on September 28, 2018, Facebook notified users who were logged out of their accounts of the Data Breach, explaining that the forced logouts were a precaution related to the Data Breach.

100. Facebook claims that it has determined that the Data Breach took place between September 14 and 27, 2018, during which time unauthorized individuals gained access to 30 million users' access tokens.[70]

101. Facebook also claims that it has fixed the vulnerability and temporarily disabled the "View As" feature, but reports suggest the vulnerability existed for over a year, from July 2017 to September 2018, before it was claimed to have been discovered.[71]

102. According to Facebook, the Data Breach compromised the following PII:

> For approximately 15 million users: name and basic contact information (phone number and/or email address).
>
> For approximately 14 million users: name, basic contact information, username, date of birth, gender, device types used to access Facebook, language selected to use Facebook in, certain other profile fields if the user had chosen to add them to their profile (relationship status, religion, hometown, self-reported current city, work, education, and website), the last 10 places the user checked into or were tagged in, the 15 most recent searches the user entered into the Facebook search bar, and the People or Pages followed by the user on Facebook.[72]

103. Facebook also admits that at minimum 70,000 users had their access tokens compromised in the Data Breach.[73] At least some of these users are California residents.[74]

104. Of the Data Breach, Zuckerberg said, "We're taking it really seriously. I'm glad we

---

https://www.facebook.com/help/securitynotice?ref=sec (last accessed Feb. 7, 2019).

[70] *Id.*

[71] Chance Miller, *How to Find Out if your Data was Included in Facebook's Latest Security Breach*, 9 TO 5 MAC (Oct. 13, 2018), *available at*: https://9to5mac.com/2018/10/13/facebook-data-breach-account-check/.

[72] "Facebook's Statement," ECF No. 61, at 6.

[75] Isaac & Frenkel, *supra* n.72.

[75] Isaac & Frenkel, *supra* n.72.

found this, but it definitely is an issue that this happened in this first place."[75]

105. Today, Facebook provides free and subscription-based resources for third-party developers and general users, which provide advice, community forums, and best practices related to privacy and security settings. These resources also serve as a medium for Facebook to promote its latest security efforts.

106. However, none of the privacy and security tools or settings Facebook provides and recommends would have prevented the Data Breach—which was the result of Facebook releasing multiple features prematurely, with vulnerabilities, and without ensuring they met industry-standard security best practices

G. Facebook Knowingly Failed to Adequately Protect Users' PII

i. Facebook's Access Tokens Were a Security Risk Because They Granted a Lot of Access and Were Easy to Exploit

107. The vast majority of Facebook users access Facebook through their mobile device. In 2019, it is estimated that 96% of all Facebook utilizes the application from a mobile device.[76]

108. Throughout development, Facebook has used many NoConfidence tokens, which are highly permissioned: i.e. they give the individual deploying them a high level of permissible actions. For instance, there are publicly-available YouTube videos[77] showing how to access a business Instagram account of a third party using a Facebook token.

109. NoConfidence tokens do not require the credentials of the end user. If an individual inserts the token into the HTML they will have access to an account even if the username and password are wrong. The token will even bypass multi-factor authentication.

---

[75] Isaac & Frenkel, *supra* n.72.

[76] *Device usage of Facebook users worldwide as of January 2019*. STATISTA, *available at* https://www.statista.com/statistics/377808/distribution-of-facebook-users-by-device/) (last accessed on July 17, 2019)

[77] *See, e.g.*, *Facebook Access Token Vulnerability - Retrieve Data via Instagram Business* (Oct. 2, 2018), *available at:* https://www.youtube.com/watch?v=tdLKRky1Da4

110. One NoConfidence token that was exposed in the Data Breach, was the FB4A token, also known as the Facebook For Android token.[78] The FB4A token was specifically designed not to expire and to persist (never expire) even if the user logged out of the application and even when the user opted out of the entire platform (i.e. removed Facebook from their device and closed their user account).

111. These tokens can be extracted with free software tools.

112. Once someone can compromise the user access token of a Facebook user the Facebook Explorer page allows that individual how to then access all tokens from the user's shared or connected web applications, such as Microsoft Azure cloud platform, SalesForce, Skype, Uber, and others.

113. In addition, anyone with access to the token can reset all other user data permissions and steal the tokens of a user's trusted third-party applications with no alert provided to the user.

114. Facebook claims that three design vulnerabilities led to the exposure of the users' access tokens.

115. Facebook has yet to make any claim that it performed basic security testing of its code or exposure-testing of its access tokens.

116. Such basic security testing is a fundamental procedure that has been considered an industry-standard best practice since 2004, and implementation of such testing would have revealed the problems which permitted the Data Breach to occur.

117. The Open Web Application Security Project ("OWASP"), the International Standards Organization ("ISO"), and the National Institute for Standards in Technology ("NIST") have all developed what are considered the global industry standards for web application security development and testing and have emphasized and reiterated the need to test for exposed cookies and access tokens that could lead to unauthorized access to secure websites.

---

[78] Facebook develops its code based upon the Android operating system, because Google made the mobile android operating system open source.

118. Cross-Site Scripting ("XSS") enables attackers to inject client-side scripts, bypass access controls such as the same-origin policy, stealing visible tokens and cookies.

119. Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.

120. XSS and CSRF have been consistently ranked in the top-ten security risks since 2004. OWASP described XSS as "the most prevalent web application security flaw" which occurs when an application includes user-supplied data without properly validating that content.[79] The detection of most XSS flaws, including flawed access tokens practices, "is fairly easy via testing or code analysis."[80]

121. XSS and CSRF are used in tandem to exploit exposed user access tokens. In the security industry, it is acknowledged and generally accepted that an exposed user access token will usually enable an attacker to impersonate a victim and illegitimately gain access to the application and thus, that victim's personal data.

122. Once a malicious actor is able to gain access to and compromise that user's access token, Facebook's lack of security and safeguards allowed that malicious actor to then use that access token to gain access to and compromise all tokens from that user's shared or connected web applications (i.e., those applications that utilize the "Facebook Login" system, such as Microsoft Azure cloud platform, SalesForce, etc.). Worse, that malicious actor could then reset all user permissions, passwords, and other safeguards (such as two-factor authentication) not only in Facebook, but also any third-party accounts that utilize Facebook's authentication login features without any additional verification and do so without alerting or notifying the users in any manner. From there, the malicious actor can siphon PII and other personal data from those accounts without hindrance. To prevent unauthorized users from eavesdropping, there is free software to

---

[79] *OWASP Top Ten Project*, OWASP, *available at*: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

[80] *Id.*

validate the data transferred between the client browser and the application servers. Most hackers also utilize the free software as a simple method to detect and identify easy areas of exploit.

ii. Facebook Knew That the Tokens Were a Security Risk and Still Chose Not to Protect Users' PII

123. Facebook's failure to adequately protect its users' tokens was exacerbated by the fact that Facebook internally knew that its access tokens were vulnerable to the kind of attack that eventually occurred, yet did nothing to prevent it.

124. Facebook had already exposed user tokens through the "View As" an impersonated user functionality back in 2014. As a result, Facebook took down the "View As" functionality and later re-introduced it in 2016 and 2017 for the benefit of user privacy. After the 2018 Data Breach, Facebook security engineer Stephen Sclafani wondered why Facebook had not caught the issue, noting "I remember looking at View As in 2016-2017. But I guess after the last issue [in 2014] I assumed that there wouldn't be a repeat."[81]

125. As early as March of 2016, Facebook recognized risks specific to the Facebook for Android token. A button clicked in the FB4A could cause an unexpected action to be taken in the Facebook Messenger application, such as a video call. This could be triggered by anyone who had an authenticated FB4A token, regardless of who originally owned the token, and regardless of whether the FB4A token matched the device on which it was created (i.e., an attacker could copy an FB4A token, inject it on a new device, and completely emulate the experience without any verification).[82]

126. Throughout 2017, members of Facebook's Product Security Team assessed issues with the Video Uploader service and test users, which appeared to have something to do with the FB4A token.[83]

127. By December of 2017, Neal Poole, a software engineer at Facebook who was part

---

[81] FB-Schmidt-000049974
[82] FB-Shmidt-000053846
[83] *See* FB-Schmidt-000052617; FB-Schmidt-000054527; FB-Schmidt-000053863

of the Product Security Team, concluded from the discussions that the Video Uploader service to shouldn't be launched to the public, noting "and I would agree, using an APIFullPermissions token for FB4A here appears misleading at best and at worst is an easy way to silently persist access as an attacker." [84] In other words, if these tokens became compromised, the attacker could access the user's profile without the user's knowledge. Furthermore, an attacker with access to an already compromised account could potentially extract the FB4A token and use it to request additional information despite no longer having physical access to the device from which it was generated.

128. In early 2018, the Product Security Team at Facebook continued to discuss concerns about the FB4A. However, Facebook continued to use highly permissioned access tokens, and did not change policies as to expirations.[85]

129. By May 2018, Facebook personnel became cognizant that the FB4A token did not expire or became invalid after a user logged out, unless the user knew to log out of *all* sessions. This was a problem because the user had no other way to invalidate the token if it was compromised. But, Facebook decided not to fix the issue because "invalidating an existing token . . . will break a lot of stuff." In a discussion among Facebook employees, Ben Yang said, "[W]e should be questioning whether this is the proper use of authentication frameworks." [86] Facebook neither changed the policy nor warned users of this risk (nor even suggested to users that they occasionally log out).

130. In early July 2018, Facebook's Product Security Team noticed an unusual increase in activity on FB4A coming from users who had no other time or activity logged on Facebook.[87]

131. Later in July 2018, Nishith Nand (another Facebook software engineer) and Neal

---

[84] FB-Schmidt-000054518
[85] FB-Schmidt-000044209
[86] FB-Schmidt-000054260
[87] FB-Schmidt-000000853

Poole discussed the security risk of the FB4A tokens, noting that "since these don't expire and don't get invalidated on a simple logout, anyone with these can potentially impersonate the user."[88] Nand also stated that there were multiple YouTube videos on how to harvest and exploit these tokens. This also shows that the public and the hacker community was aware of the value (and vulnerability) of these tokens.

132. The development team was unwilling to make changes to the FB4A token due to concern that it would break workflows, thus disrupting Facebook's ability to generate revenue—Facebook chose money over security.[89]

133. Facebook also knew that changing legacy code and eliminating NoConfidence tokens (like the FB4A token) altogether would be expensive and, again, disrupt or curtail their advertising revenue and third party paid subscribers.

134. Furthermore, despite Facebook's tools and ability to search through its code for flaws and also to capitalize on reusable code to expedite new features and functionalities, Facebook never once exhibited a desire to search through its code for security flaws or trace the use and attempt to secure or protect the use of NoConfidence tokens. At the same time, Facebook highly encouraged third party games, services, applications to use Facebook's authentication mechanisms, including the NoConfidence FB4A token.

135. Typically, linking two sites through authentication allows both sites to share profile and other data about the user. However, in the case of NoConfidence, persistent (never expiring) tokens, it also allowed Facebook to track user behavior for target marketing and accumulate vast amounts of behavioral profiling on its users, and on any individuals who did not have a Facebook account but used a game or application that was authenticated through Facebook.

136. In early September of 2018, Facebook received a tweet from a non-employee

---

[88] FB-Schmidt-000054545

[89] *See* FB-Schmidt-000045722; FB-Schmidt-000046524

regarding vulnerabilities. However, Facebook's did not react until September 29, 2018.[90]

137. On September 7, 2018, Facebook employee Penny Wu was notified that a business employee was able to view various information he should not have access to with a FB4A token.[91]

138. After the Data Breach was detected and announced, several Facebook employees discussed their neglect of the access token vulnerability, specifically after they saw the increase in unusual activity on the FB4A in early July 2018. In discussions among Facebook employees, Joseph Adler noted, "We had planned to migrate this access token issue but it was never done. We are trying to figure out how exactly the exploit is done and how many users and IPs were involved." Another employee, Steve DeLucia noted, "But we have seen abuse vectors like this in the past for other Facebook apps."[92]

139. On September 26, 2018, Facebook employee Ben Yang noted, "**it hurts knowing that if our stuff was done faster/in a better state this could have been prevented.**" (emphasis added). Neal Poole responded with an acknowledgment of the admission and an old-school emoji: "Yeah :-(". Yang replied, "wonderful, this is something I worked on but didn't finish; the guilt really decided to sucker punch me on this one."[93]

140. On November 12, 2018, another Facebook employee, Kyle Minshall remarked "It's pretty common for FB4A access tokens to be used for scraping because they're full permission and are not affected by rate limiting. Very common attack vector."[94]

141. In the initial investigation after the Data Breach, Facebook discovered that Facebook Messenger, Facebook Ad Payments, Instagram and many other areas were affected, but chose to limit the investigation. During the remediation and mitigation process that followed, Facebook purposely limited all non-employee investigations to only the time period in which the

---

[90] FB-Schmidt-000052079
[91] FB-Schmidt-000054471
[92] FB-Schmidt-000053844
[93] FB-Schmidt-000052491
[94] FB-Schmidt-000055983

hackers were detected and to the behavior of the hackers that were caught. [95]

142. There is no evidence presented that the legacy "View As" code was tested prior to re-release in 2016-2017. In addition, there is no evidence that the Video Uploader code was security tested.

H. Facebook's Lax Security Resulted in Yet Another Breach

143. In December of 2018, Facebook had another security breach.[96] A flaw allowed third-party application providers to see, through the social network's "Facebook Login" system, photos that had been uploaded but not published on Facebook, as well as photos published to Facebook's "Marketplace" and to its Stories feature. The bug also impacted photos that people uploaded to Facebook but chose not to post. Facebook said the breach "affected up to 6.8 million users and up to 1,500 apps built by 876 developers."

144. The photo vulnerability was initially introduced on September 13, 2018—meaning developers could have accessed users' photos for 12 days.[97] Like the user access token flaw, this vulnerability demonstrates a failure to test and correct flaws before launch. It also shows that Facebook relies on the public to find the bugs that Facebook itself missed.

I. Impacted Users Have Been Greatly Harmed and Face Significant Ongoing Risks as a Result of the Data Breach.

145. There are serious implications related to the theft of access tokens, including that someone with a user's token can access a user's account (including any applications the user is logged into via Facebook) and impersonate the user online. This would enable unauthorized individuals not only to download the entire archive of personal and profile data to use at any time in the future, including all historical account activity and private messages sent and received by the

---

[95] FB-Schmidt-000043121

[96] Michael Cappetta, *Facebook Apologizes After Security Flaw Exposes Unpublished Photos*, NBC NEWS (Dec. 14, 2018), *available at*: https://www.nbcnews.com/tech/security/facebook-apologizes-after-security-flaw-exposes-unpublished-photos-n948051.

[97] *Id.*

user since the account was created, but also send messages from a user's account and send and request money to other users through Facebook Payments.[98]

146. Further, it appears that the Data Breach impacted Facebook Login, which permits users to use their Facebook accounts and credentials to sign into accounts with third parties such as Netflix, Ancestry.com, ESPN, and Spotify.[99]

147. There are tens of thousands of additional websites and services (including apps, online retailers, and games) that permit Facebook users to take advantage of a "Login with Facebook" feature including: Instagram and WhatsApp (both owned by Facebook), Uber, eBay, LinkedIn, dating websites, Airbnb, and Yelp.

148. With access to the user tokens, unauthorized users could also take over these accounts and use them as if they were the accountholders without having to enter a password.

149. Activities could include accessing personal and private information—including photos, personal messages, search histories, purchase histories, professional networks and job-search information; accessing information that could compromise the users' safety, including travel and lodging plans, routine travel routes, and frequently visited addresses, including home and work; changing permissions and privacy settings; posting or viewing information shared by those accounts and any users connected to them; and accessing financial information.

150. Facebook noted the attackers were from a known group it was watching, and thus the attack was foreseeable.

151. Facebook has attempted to minimize the hack, claiming (without evidence) that the unauthorized individuals who gained access to users' accounts "were spammers looking to make money through deceptive advertising . . . that present themselves as a digital marketing company, and whose activities were previously known to Facebook's security team . . ."[100]

---

[98] Allen St. John, *supra* n.7.

[99] *Id.*

[100] Robert McMillan & Deepa Seetharaman, *Facebook Finds Hack Was Done By Spammers, Not*

152. While Facebook claims that it has fixed the problem, that seems unlikely for impacted users. While Facebook forcibly logged approximately 90 million users out of their accounts to reset the access tokens that permitted unauthorized individuals to access PII during the Data Breach, that reset does not log users out of all active sessions; in other words, if a user was logged out of her active session on her iPhone with the Facebook application, that user may not have been logged out of other devices, such as her tablet, laptop, or desktop computers that also had Facebook sessions active.

153. In fact, Facebook leaves users logged in to unused apps (e.g., the app on the user's tablet) unless and until the user logs out.

154. This is particularly true for mobile devices, which account for 96% of all active Facebook users.[101]

155. Active sessions may also be open on devices long abandoned by the users, such as an iPhone that a user subsequently replaced, and which is now in the possession of a third party.

156. To log out of all active sessions, Facebook users must take additional steps and drill through their "Settings" menu and elect to "Log Out of All Sessions" through their account. Without completing this step—and possibly even with this additional step—unauthorized individuals may still have access to users' profiles to continue to take PII in connection with the Data Breach.[102]

157. Further, the reset did not address the "Facebook Login" issue and does not protect

---

Foreign State. THE WALL STREET JOURNAL (Oct. 17, 2018), available at: https://www.wsj.com/articles/facebook-tentatively-concludes-recent-hack-was-perpetrated-by-spammers-1539821869

[101] *See, e.g.*, STATISTA, *supra* n.82; *see also* Napier Lopez, *90% of Facebook's Daily Active Users access it via Mobile*, THE NEXT WEB (Jan. 27, 2016), *available at*: https://thenextweb.com/facebook/2016/01/27/90-of-facebooks-daily-and-monthly-active-users-access-it-via-mobile/; *Share of Facebook users worldwide who accessed Facebook via Mobile from 2013 to 2018*, STATISTA, *available at*: https://www.statista.com/statistics/380550/share-of-global-mobile-facebook-users/.

[102] Anna Brading, *Big Facebook data breach: 50 million accounts affected*, NAKED SECURITY BY SOPHOS (Sept. 28, 2018), *available at*: https://nakedsecurity.sophos.com/2018/09/28/big-facebook-breach-50-million-accounts-affected/.

users whose tokens were already stolen or whose information was already accessed.

158. The information in a Facebook account contains, at a minimum, all posts, photos and videos, all replies, likes and reactions, all friends and friend history, all games, every "follow" including individuals, event, activity, service, application, group, web sites, advertisements, all followers of the same, all messages exchanges, event RSVPs, all profile information (username, devices, authentication methods, recoverable email accounts and credentials, encryption settings, phone numbers, challenge response information, biometric information and settings, birth date, major events, employment, education, education history, personal preferences, "about me," religion and political preferences, work history, book preferences, fitness data, news feed preferences, musical preferences), GPS locations where messages, photos, and posts were made, all "pokes," all advertisements, all calls and messages and associated event logs, and all security and login information including all devices used to access Facebook.

159. This stolen data is valuable to wrongdoers, who can use the information taken for, *inter alia*, "knowledge-based authentication"—which is important to setting up and breaking into accounts.[103]

160. For instance, banks and other holders of PII use personal data to safeguard accounts, including information such as a consumer's mother's maiden name, pets' names, or the street the consumer grew up on.

161. As a result of the Data Breach, such authentication information is now in the hands of unauthorized individuals who can use it to access or create accounts and circumvent the safeguards based on consumers' compromised personal data.

162. Persistent or immutable identifiers (data generally associated with an individual for life), such as date of birth, family names, someone's hometown, high school, etc. are especially

---

[103] Dave Lee, *Facebook hack victims will not get ID theft protection*, BBC NEWS (Oct. 12, 2018), *available at*: https://www.bbc.com/news/technology-45845431.

useful to criminals for many damaging forms of identity misuse, including new account fraud, tax fraud, and the release of logins or passwords for individuals to individuals who claim to have lost them.[104] Since forgotten logins and passwords are a frequent request at customer service desks, these types of immutable identifiers are commonly used to grant access to bank, healthcare, and other sensitive accounts—which can in turn enable the hacker to take over an account or commit other types of fraud or harm.[105]

163. In addition, even non-immutable identifiers put individuals at prolonged risk for identity misuse. For instance, on average, individuals have the same home address for 7 years.[106] Both such identifiers can be valuable to criminals for gaining additional PII, in order to successfully commit identity fraud. Street addresses can allow criminals to pilfer PII found in sensitive documents such as financial statements or checks, from physical mailboxes. Identity criminals rely on a wide manner of interaction channels for communicating with victims, including telephone, email and physical mail.[107] Any communication channel—from door-to-door, phone and digital—may be used as an interaction method for social engineering that enables criminals to impersonate a trusted third party, gain additional PII, and thus commit fraud.

164. Further, so-called "phishing" schemes seeking to extort money appear more legitimate to the targeted victim when a cybercriminal employs PII in the scheme.

165. Phishing schemes have a much greater likelihood of success when personal, non-public information is used to spoof or fool the recipient.

---

[104] *5 Ways To Solve The Password Reset Problem*, DARK READING, http://www.darkreading.com/attacks-and-breaches/5-ways-to-solve-the-password-resetproblem/d/d-id/1105781?piddl_msgid=324276#msg_324276, Aug 14, 2016

[105] *See The 10 Most Common IT Service Desk Requests*, https://blog.samanage.com/help-desksoftware/the-10-most-common-service-desk-requests-2/, September 25, 2013.

[106] How Many Times Does The Average Person Move? http://fivethirtyeight.com/datalab/how-manytimes-the-average-person-moves/ Accessed November 28, 2016

[107] Consumer Sentinel Network Data Book for January-December 2015, Federal Trade Commission, February 2016, page 3.

166. The Data Breach also makes users susceptible to ransomware or blackmailing attacks, because people use Facebook to "talk about things they wouldn't want their employer or their spouse to know. Hackers can do nasty stuff with that." [108]

167. This information is found in, for example, users' private messages and in their Facebook-connected web services.

168. For example, Microsoft's Azure cloud platform is a connected web service that uses Facebook to authenticate logins (i.e., a user uses her or his Facebook account to login to the service, instead of using a username and password provided by the connected web service). With access to Microsoft's Azure cloud platform via the user's Facebook credentials, an unauthorized third party then has access to that user's account and can continue to exfiltrate data beyond the PII Facebook stored.

169. The Microsoft Azure cloud platform login is not the only example where users may utilize Facebook's authentication login feature. SalesForce, Skype, Uber, and myriad services use this Facebook's authentication login feature. Thus, the Facebook user's compromised token serves not only as a digital key to the Facebook platform, but also any other service that user connected to Facebook's authentication login feature.

170. The Electronic Frontier Foundation has noted that the type of information exposed in the Data Breach is "extra-valuable to criminals" given that it is highly accurate, having been entered by users themselves, whereas personal information stolen from prior data breaches was inferred from consumer behavior.[109]

171. Despite its clear misfeasance in protecting consumers from unlawful data breaches and the significant harms consumers face as a result, Facebook has already announced that it will not be providing the bare minimum relief that many companies provide after a breach—identity

---

[108] Allen St. John, *supra* n.7.
[109] *Id.*

theft protection services.[110]

172. Moreover, although Facebook users were notified within the application that they their PII was compromised in the Data Breach, Facebook does not appear to have provided any notifications outside of the Facebook platform.

173. Thus, if a user has a dormant Facebook profile she or he never uses, or the user deleted her or his Facebook profile leading up to the Data Breach but the user's profile still existed on Facebook's servers, those individuals did not receive any notification concerning the compromise of their PII. Notwithstanding possessing those individuals' emails, phone numbers, and other information sufficient to identify and notify the users, Facebook's efforts ceased with notifications within the Facebook platform, and no efforts have been made to use that contact information to inform users that their PII was compromised.

174. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. [111] Annual subscriptions for credit monitoring plans range from $219 to $329 per year.[112]

J. Plaintiff's Experience

175. Plaintiff Stephen Adkins is a resident of the state of Michigan.

176. Plaintiff Adkins has been a Facebook User since March 4, 2009.

177. Plaintiff Adkins provided Defendant with PII including his name, email address, telephone number, date of birthday, locations, work and education history, and photographs.

178. On October 12, 2018, Plaintiff Adkins saw a news article online discussing the Facebook data breach and attempted to access his account, however he had been forcibly logged out. Plaintiff Adkins was required to create a new password to log in.

179. Once he logged back in to his account, Plaintiff Adkins received a notification at the

---

[110] *Id.*
[111] *See* Plaintiff's March 7, 2019 Amended Initial Disclosures pursuant to Rule 26(a) at p. 25.
[112] *Id.*

top of his Facebook NewsFeed discussing the breach.

180. Plaintiff Adkins visited the "Security Incident" Facebook page related to his account, and was informed that the following categories of information have been compromised: name, primary email address, most recently added phone number, username, date of birth, gender, types of devices used to access Facebook, language preference, relationship status, religion, hometown, current city, work, education, website, 10 most recent locations he checked into or had been tagged in, 15 most recent searches he entered into the Facebook search bar, and People or Pages he follows on Facebook.

181. As a result of the 2018 Data Breach, Plaintiff Adkins had difficulty logging back into his Facebook account, and received dozens of "phishing" email messages.

182. Plaintiff Adkins spent time dealing with the consequences of the Data Breach, which includes time spent dealing with phishing emails and time spent canceling and changing the credit card he believed to be associated with his Facebook account.

183. Knowing that a hacker has his information had caused Plaintiff Adkins great anxiety, so much so that for him "it's scary to even think about" all the information a hacker might have.[113]

184. Following the Data Breach, in or around October 2018, Plaintiff Adkins researched credit monitoring services from LifeLock but did not purchase them because he could not afford them.[114]

185. Plaintiff Adkins intended to and did participate in the online information exchange market in which PII functions as money paid for the use of social media platforms and other online services.

186. Plaintiff Adkins chose where he spent his PII. For instance, in addition to Facebook, he exchanged his PII for services such as Yelp, Twitter, Skype, Periscope, Amazon, Yahoo, Cash,

---

[113] May 9, 2019 Deposition of Stephen Adkins ("Adkins Depo.") at 424:2-7.
[114] *Id*. at 267:10–268:13.

PlentyOfFish (a dating website), Pandora, MyFitnessPal—all of which rely on PII to generate advertising revenue.[115]

187. Now, due to Facebook's misconduct and the resulting Data Breach, hackers obtained his PII at no compensation to Plaintiff whatsoever. That is money lost for Plaintiff Adkins, and money gained for the hackers, who could sell the PII for $15-30 on the Dark Web market.

CLASS ALLEGATIONS

188. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 187.

189. Plaintiff brings this nationwide class action pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class (the "Nationwide Class"):

> **All Facebook users whose PII was compromised in the data breach announced by Facebook on September 28, 2018.**

190. Excluded from the Class are the following individuals and/or entities: Defendant and its parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

191. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

192. **Numerosity**: The Class is so numerous that joinder of all members is impracticable. Facebook has identified millions of Facebook users whose PII was accessed in the Data Breach, and

---

[115] *See* Adkins Depo. at 171:21-22; 166:2-9; 163:13-14; 163:23-24; 30:2-3; 134:7-8 171:15-16; 170:25-171:5; 165:5-12; 28:5-9.

the Class is apparently identifiable within Facebook's records.

193. **Commonality**: Questions of law and fact common to the Class exist and predominate over any questions affecting only individual class members. These include:

a. Whether and when Facebook learned of the Data Breach and whether its response was adequate;

b. Whether Facebook owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;

c. Whether Facebook breached that duty;

d. Whether Facebook implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class members' PII;

e. Whether Facebook acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class members' PII;

f. Whether Facebook knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class members' PII secure and prevent loss or misuse of that PII;

g. Whether Facebook adequately addressed and fixed the "View As" vulnerabilities which permitted the Data Breach to occur;

h. Whether Facebook caused Plaintiff and Class members damages; and

i. Whether Plaintiff and the other Class members are entitled to credit monitoring, and other monetary relief.

194. **Typicality**: Plaintiff's claims are typical of those of other Class members because all had their PII compromised accessed as a result of the Data Breach, due to Facebook's misfeasance.

195. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating privacy-related class actions.

196. **Superiority and Manageability**: Under 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the

members of the Class is impracticable. Individual damages for any individual Class member are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action. The Terms of Service for Facebook accounts requires all "Disputes" be governed by "the laws of California" that further facilitates a nationwide class action.[116]

197. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

198. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and the Class members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and the Class members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

---

[116] *Terms of Service*, Facebook, Inc., https://www.facebook.com/terms.php (last accessed Feb. 7, 2019).

e. Whether Class members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I

NEGLIGENCE

199. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 187.

200. Facebook owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

201. The legal duties owed by Defendant to Plaintiff and Class members include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiff and Class members in its possession;

b. To protect PII of Plaintiff and Class members in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Class members of the Data Breach.

202. In addition, Cal. Civ. Code §1798.81.5 requires Facebook to take reasonable steps and employ reasonable methods of safeguarding the PII of Class members who are California residents.

203. Facebook's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the FTC, the unfair practices of failing to use reasonable measures to protect PII by companies such as Facebook.

Various FTC publications and data security breach orders further form the basis of Facebook's duty.[117] Various FTC publications and orders also form the bases of Facebook's duty. Plaintiff and Class members are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, the previous consent decree by the FTC regarding user privacy, and the Cambridge Analytica theft of user data for which Facebook had just recently apologized.

204. In addition, given the nature of the information, Facebook had a special relationship with Plaintiff and the Class members. Plaintiff and the Class members signed up for Facebook's services and agreed to provide their PII with the understanding that Facebook would undertake to safeguard the PII and would promptly inform Plaintiff and the Class of any privacy intrusions that might compromise the PII which it represented it would maintain privately and safely. There representations by Facebook induced Plaintiff and Class members to disclose PII in their profiles.

205. Facebook breached its duties to Plaintiff and Class members. Facebook knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems.

206. Facebook knew or should have known that its security practices did not adequately safeguard Plaintiff's and the other Class members' PII, including, but not limited to, the failure to include expirations on access tokens.

207. As stated herein, including specifically Paragraphs 107-141, for over two years leading up to the attack, key Facebook personnel knew that there were serious vulnerabilities with access tokens. Facebook employees repeatedly raised the issue of the token's potential for being exploited. Yet despite all that Facebook refused to make changes to the tokens or even warn users.

---

[117] See, e.g., *Data Protection: Actions taken by Equifax and Federal Agencies in Response to the 2017 Breach*, UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE (Aug. 30, 2019), *available at*: https://www.gao.gov/products/GAO-18-559 (regarding the Equifax data breach).

Unsurprisingly, after the breach, Facebook employees expressed "guilt" and acknowledged that not only did they know about this security risk, but had they worked faster and better, the Data Breach "could have been prevented."

208. Through Facebook's acts and omissions described in this Complaint, including Facebook's failure to provide adequate security and its failure to protect the PII of Plaintiff and the Class from being foreseeably captured, accessed, exfiltrated, stolen, and misused, Facebook unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' PII during the period it was within Facebook's possession and control.

209. Facebook breached the duties it owes to Plaintiff and Class members in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect Facebook users' PII and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the data breach;

c. Failing to act despite knowing or having reason to know that the access tokens were a security vulnerability and

d. Failing to timely and accurately disclose to Facebook users that their PII had been improperly acquired or accessed.

210. Because the limitation-of-liability clause does not mention "negligence" at all, let alone unequivocally preclude liability for it, the provision is also unenforceable against Plaintiff's negligence claim.

211. Due to Defendant's conduct, Plaintiff and Class Members are entitled to credit monitoring. Credit monitoring is reasonable here. The PII taken is historical and can be used towards identity theft and other types of financial fraud against the Class Members. There is no question that this PII was taken by sophisticated cybercriminals increasing the risks to the Class Members. The consequences of identity theft are serious and long-lasting. There is a benefit to early detection and monitoring. Some experts recommend that data breach victims obtain credit monitoring services for

at least ten years following a data breach. [118] Annual subscriptions for credit monitoring plans range from $219 to $329 per year.[119]

212. As a result of Defendant's negligence, Plaintiff and Class members suffered injuries, that may include (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised Facebook account; (iv) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in their continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members, including ongoing credit monitoring.

213. These injuries were reasonably foreseeable given the history of security breaches at Facebook, detailed above and the purported high number of attempted data breaches it and other similar social media providers face daily. Facebook even claims that the hackers are a digital marketing company "whose activities were previously known to Facebook's security team."[120]

214. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Facebook's negligent conduct.

COUNT II

DECLARATORY JUDGMENT

215. Plaintiff re-alleges and incorporates by reference herein all of the allegations

---

[118] *See* Plaintiff's March 7, 2019 Amended Initial Disclosures pursuant to Rule 26(a) at p. 25.
[119] *Id.*
[120] Robert McMillan & Deepa Seetharaman, *supra* n.110.

contained in paragraphs 1 through 187.

216. Defendant owes duties of care to Plaintiff and Class members which would require it to adequately secure PII.

217. Defendant still possesses PII regarding Plaintiff and Class members.

218. Although Facebook claims it has identified who was harmed by the breach and the extent and corrected the vulnerabilities in its systems which permitted the intrusions to prevent further attacks, there is no detail on what, if any, fixes have occurred.

219. Plaintiff and Class members are at risk of harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

220. There is no reason to believe that Defendant's security measures are any more adequate than they were before the breach to meet Defendant's contractual obligations and legal duties, and there is no reason to think Defendant has no other security vulnerabilities that have not yet been knowingly exploited. Defendant faced security breaches, conducted an "apology tour" before Congress and many media outlets, and then this breach occurred, followed by another announced in December 2018.

221. Plaintiff, therefore, seeks a declaration that (1) Facebook's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide adequate security, and (2) to comply with its explicit or implicit contractual obligations and duties of care, Facebook must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Facebook' systems on a periodic basis, and ordering Facebook to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Facebook audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Facebook user applications be segmented by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Facebook conduct regular database scanning and securing checks;

f. Ordering that Facebook routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Ordering Facebook to purchase credit monitoring services for Plaintiff and Class members; and

h. Ordering Facebook to meaningfully educate its users about the threats they face as a result of the loss of their financial and Private Information to third parties, as well as the steps Facebook users must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class members, requests judgment against the Defendant and that the Court grant the following:

A. An order certifying a class or classes and appointing Plaintiff and his Counsel to represent the Class;

B. An order enjoining Facebook from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiff's and Class members' PII;

C. An order instructing Facebook to purchase or provide funds for credit monitoring services for Plaintiff and all Class members;

D. An award of compensatory, statutory, and punitive damages, in an amount to be determined;

E. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

F. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff hereby demands a jury trial for all issues so triable of right.

DATED this 16th day of August, 2019.

Respectfully submitted,

s/ *Andrew N. Friedman*

Andrew N. Friedman (*Pro Hac Vice*)
afriedman@cohenmilstein.com
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave. NW
East Tower, 5th Floor
Washington, DC 20005
Telephone: (202) 408-4600
Facsimile: (202) 408-4699

John A. Yanchunis (*Pro Hac Vice*)
jyanchunis@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
T: 813-223-5505
F: 813-223-5402 (fax)

Ariana J. Tadler (*Pro Hac Vice*)
atadler@TadlerLaw.com
TADLER LAW LLP
One Penn Plaza
New York, New York
New York, NY 10119
Telephone: (212) 946-9453
Facsimile: (212) 273-4375

Attorneys for Plaintiff

CAPSTONE LAW, APC
Tarek H. Zohdy (SBN 247775)
Tarek.Zohdy@capstonelawyers.com
Cody R. Padgett (SBN 275553)
Cody.Padgett@capstonelawyers.com
Trisha K. Monesi (SBN 303512)
Trisha.Monesi@capstonelawyers.com
Capstone Law APC

1875 Century Park East, Suite 1000
Los Angeles, California 90067
Telephone: (310) 556-4811
Facsimile: (310) 943-0396

CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
David S. Casey, Jr. (SBN 060768)
dcasey@cglaw.com
Gayle M. Blatt (SBN 122048)
gmb@cglaw.com
Jeremy Robinson (SBN 188325)
jrobinson@cglaw.com
110 Laurel Street
San Diego, California 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232 fax

CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORPORATION
Clayeo C. Arnold (SBN 65070)
carnold@justice4you.com
Joshua H. Watson (SBN 238058)
jwatson@justice4you.com
865 Howe Avenue
Sacramento, California 95825
Telephone: 916-777-7777
Facsimile: 916-924-1829

COHEN MILSTEIN SELLERS & TOLL PLLC
Douglas J. McNamara
dmcnamara@cohenmilstein.com
Karina G. Puttieva (SBN 317702)
kputtieva@cohenmilstein.com
1100 New York Ave. NW
East Tower, 5th Floor
Washington, DC 20005
Telephone: (202) 408-4600
Facsimile: (202) 408-4699

FINKELSTEIN, BLANKENSHIP, FREI-PEARSON & GARBER LLP
Jeremiah Frei-Pearson
Jfrei-pearson@fbfglaw.com
Andrew C. White
awhite@fbfglaw.com
445 Hamilton Ave., Suite 605
White Plains, New York 10601
Telephone: (914) 298-3281
Facsimile: (914) 908-6709

FRANKLIN D. AZAR & ASSOCIATES
Ivy Ngo (SBN 249860)
ngoi@fdazar.com
Kelly Hyman
hymank@fdazar.com
14426 East Evans Ave
Aurora, CO 80014
Telephone: 303-757-3300
Facsimile: 720-213-5131

GLANCY PRONGAY & MURRAY LLP
Marc Godino
mgodino@glancylaw.com
Brian Murray
bmurray@glancylaw.com
1925 Century Park East, Suite 2100
Los Angeles, California 90067
Telephone: 310-201-9150
Facsimile: 310-432-1495

JONES WARD PLC
Jasper D. Ward
jasper@jonesward.com
1205 E Washington St, Suite 111
Louisville, Kentucky 40206
Telephone: 502-882-6000

KANTROWITZ GOLDHAMER & GRAIFMAN, P.C.
Gary S. Graifman
ggraifman@kgglaw.com
Jay Brody
jbrody@kgglaw.com
747 Chestnut Ridge Road
Chestnut Ridge, New York 10977
Telephone: (845) 356-2570
Facsimile: (845) 356-4335

KOHN, SWIFT & GRAF, P.C.
Jonathan Shub (SBN 237708)

jshub@kohnswift.com
Kevin Laukaitis
klaukaitis@kohnswift.com
1600 Market Street, Suite 2500
Philadelphia, PA 19103-7225
Telephone: (215) 238-1700
Facsimile: (215) 238-1968

LAW OFFICE OF PAUL C. WHALEN, P.C.
Paul C. Whalen
paul@paulwhelan.com
768 Plandome Road
Manhasset, NY 11030
Telephone: (516) 426-6870
Facsimile: (212) 658-9685

LAW OFFICES OF CHARLES REICHMANN
Charles Reichmann
Cpreichmann@yahoo.com
16 Yale Circle
Kensington, CA 94708
Telephone: (415) 373-8849

LOCKRIDGE GRINDAL NAUEN PLLP
Karen Hanson Riebel
khriebel@locklaw.com
Kate M. Baxter-Kauf
kmbaxter-kauf@locklaw.com
Arielle S. Wagner
aswagner@locklaw.com
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 596-4097
Facsimile: (612) 339-0981

MIGLIACCIO & RATHOD LLP
Nicholas A. Migliaccio
nmigliaccio@classlawdc.com
Jason S. Rathod
jrathos@classlawdc.com
412 H Street N.E., Ste. 302
Washington, DC 20002
Telephone: (202) 470-3520

TADLER LAW LLP
Ariana J. Tadler (*pro hac vice*)
ATadler@Tadlerlaw.com
One Penn Plaza
New York, New York
New York, NY 10119
Telephone: (212) 946-9453
Facsimile: (212) 273-4375

MORGAN & MORGAN COMPLEX LITIGATION GROUP
Ryan J. McGee
rmcgee@ForThePeople.com
Jean S. Martin
jeanmartin@ForThePeople.com
Kenya J. Reddy
kreddy@forthepeople.com
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

ROBINSON CALCAGNIE, INC.
Daniel S. Robinson (SBN 244245)
drobinson@robinsonfirm.com
Wesley K. Polischuk (SBM 254121)
wpolischuk@robinsonfirm.com
Michael W. Olson (312857)
19 Corporate Plaza Drive
Newport Beach, California 92660
Telephone: (949) 720-1288
Facsimile: (949) 720-1292

STULL, STULL & BRODY
Patrice L. Bishop (SBN 182256)
pbishop@ssbla.com
Melissa R. Emert
memert@ssbny.com
9430 W. Olympic Blvd., Suite 400
Beverly Hills, CA 90212
Telephone: (310) 209-2468
Facsimile: (310) 209-2087

Other Plaintiff's Counsel