

**POMERANTZ LLP**

Jennifer Pafiti (SBN 282790)  
468 North Camden Drive  
Beverly Hills, CA 90210  
Telephone: (818) 532-6499  
E-mail: jpafiti@pomlaw.com

**Attorney for Plaintiff**

- additional counsel on signature page -

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

FAN YUAN, Individually and on Behalf of All  
Others Similarly Situated,

Plaintiff,

vs.

FACEBOOK, INC., MARK E.  
ZUCKERBERG and DAVID M. WEHNER,

Defendants

Case No.

**CLASS ACTION COMPLAINT FOR  
VIOLATION OF THE FEDERAL  
SECURITIES LAWS**

JURY TRIAL DEMANDED

Plaintiff Fan Yuan (“Plaintiff”), individually and on behalf of all other persons similarly situated, by Plaintiff’s undersigned attorneys, for Plaintiff’s complaint against Defendants (defined below), alleges the following based upon personal knowledge as to Plaintiff and Plaintiff’s own acts, and information and belief as to all other matters, based upon, *inter alia*, the investigation conducted by and through Plaintiff’s attorneys, which included, among other things, a review of the Defendants’ public documents, conference calls and announcements made by Defendants, United States Securities and Exchange Commission (“SEC”) filings, wire and press releases published by and regarding Facebook, Inc. (“Facebook” or the “Company”), analysts’ reports and advisories about the Company,

1 and information readily obtainable on the Internet. Plaintiff believes that substantial evidentiary support  
2 will exist for the allegations set forth herein after a reasonable opportunity for discovery.

### 3 **NATURE OF THE ACTION**

4 1. This is a federal securities class action on behalf of a class consisting of all persons other  
5 than Defendants who purchased or otherwise acquired common shares of Facebook between February  
6 3, 2017 and March 19, 2018, both dates inclusive (the “Class Period”). Plaintiff seeks to recover  
7 compensable damages caused by Defendants’ violations of the federal securities laws and to pursue  
8 remedies under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 (the “Exchange Act”)  
9 and Rule 10b-5 promulgated thereunder.  
10

11 2. Facebook operates a social networking website that allows people to communicate with  
12 their family, friends, and coworkers. Facebook develops technologies that facilitate the sharing of  
13 information, photographs, website links, and videos. Facebook users have the ability to share and  
14 restrict information based on their own specific criteria. By the end of 2017, Facebook had more than  
15 2.2 billion active users.  
16

17 3. Founded in 2004, the Company is headquartered in Menlo Park, California. The  
18 Company’s common stock trades on the NASDAQ Global Select Market (“NASDAQ”) under the  
19 ticker symbol “FB.”  
20

21 4. Throughout the Class Period, Defendants made materially false and misleading  
22 statements regarding the Company’s business, operational and compliance policies. Specifically,  
23 Defendants made false and/or misleading statements and/or failed to disclose that: (i) Facebook violated  
24 its own purported data privacy policies by allowing third parties to access the personal data of millions  
25 of Facebook users without the users’ consent; (ii) discovery of the foregoing conduct would foreseeably  
26 subject the Company to heightened regulatory scrutiny; and (iii) as a result, Facebook’s public  
27 statements were materially false and misleading at all relevant times.  
28









1 25. In the 2016 10-K, with respect to the disclosure of user data, the Company merely  
2 offered the following non-specific representation:

3 ***Security breaches and improper access to or disclosure of our data or user data,***  
4 ***or other hacking and phishing attacks on our systems, could harm our***  
***reputation and adversely affect our business.***

5 Our industry is prone to cyber-attacks by third parties seeking unauthorized  
6 access to our data or users' data. Any failure to prevent or mitigate security  
7 breaches and improper access to or disclosure of our data or user data could result  
8 in the loss or misuse of such data, which could harm our business and reputation  
9 and diminish our competitive position. In addition, computer malware, viruses,  
10 social engineering (predominantly spear phishing attacks), and general hacking  
11 have become more prevalent in our industry, have occurred on our systems in the  
12 past, and will occur on our systems in the future. As a result of our prominence, we  
13 believe that we are a particularly attractive target for such breaches and attacks.  
14 Such attacks may cause interruptions to the services we provide, degrade the user  
15 experience, cause users to lose confidence and trust in our products, or result in  
16 financial harm to us. Our efforts to protect our company data or the information we  
17 receive may also be unsuccessful due to software bugs or other technical  
18 malfunctions; employee, contractor, or vendor error or malfeasance; government  
19 surveillance; or other threats that evolve. In addition, third parties may attempt to  
20 fraudulently induce employees or users to disclose information in order to gain  
21 access to our data or our users' data. Although we have developed systems and  
22 processes that are designed to protect our data and user data, to prevent data loss,  
23 and to prevent or detect security breaches, we cannot assure you that such  
24 measures will provide absolute security.

25 In addition, some of our developers or other partners, such as those that help  
26 us measure the effectiveness of ads, may receive or store information provided by  
27 us or by our users through mobile or web applications integrated with Facebook.  
28 We provide limited information to such third parties based on the scope of services  
provided to us. However, if these third parties or developers fail to adopt or adhere  
to adequate data security practices, or in the event of a breach of their networks,  
our data or our users' data may be improperly accessed, used, or disclosed.

Affected users or government authorities could initiate legal or regulatory  
actions against us in connection with any security breaches or improper disclosure  
of data, which could cause us to incur significant expense and liability or result in  
orders or consent decrees forcing us to modify our business practices. Any of these  
events could have a material and adverse effect on our business, reputation, or  
financial results.

26 26. The 2016 10-K contained signed certifications pursuant to SOX by the Individual  
27 Defendants, stating that the information contained in the 2016 10-K "fairly presents, in all material  
28

1 respects, the financial condition and results of operations of the Company for the periods presented  
2 therein.”

3 27. On May 4, 2017, Facebook filed a quarterly report on Form 10-Q with the SEC,  
4 announcing the Company’s financial and operating results for the quarter ended March 31, 2017 (the  
5 “1Q 2017 10-Q”). For the quarter, Facebook reported net income of \$3.05 billion, or \$1.04 per diluted  
6 share, on revenue of \$8.03 billion, compared to net income of \$1.73 billion, or \$0.60 per diluted share,  
7 on revenue of \$5.38 billion for the same period in the prior year.

8  
9 28. In the 1Q 2017 10-Q, the Company again offered only a non-specific representation  
10 concerning data security:

11 ***Security breaches and improper access to or disclosure of our data or user data,***  
12 ***or other hacking and phishing attacks on our systems, could harm our***  
13 ***reputation and adversely affect our business.***

14 Our industry is prone to cyber-attacks by third parties seeking unauthorized  
15 access to our data or users’ data or to disrupt our ability to provide service. Any  
16 failure to prevent or mitigate security breaches and improper access to or  
17 disclosure of our data or user data could result in the loss or misuse of such data,  
18 which could harm our business and reputation and diminish our competitive  
19 position. In addition, computer malware, viruses, social engineering  
20 (predominantly spear phishing attacks), and general hacking have become more  
21 prevalent in our industry, have occurred on our systems in the past, and will occur  
22 on our systems in the future. As a result of our prominence, we believe that we are  
23 a particularly attractive target for such breaches and attacks. Such attacks may  
24 cause interruptions to the services we provide, degrade the user experience, cause  
25 users to lose confidence and trust in our products, or result in financial harm to us.  
26 Our efforts to protect our company data or the information we receive may also be  
27 unsuccessful due to software bugs or other technical malfunctions; employee,  
28 contractor, or vendor error or malfeasance; government surveillance; or other  
threats that evolve. In addition, third parties may attempt to fraudulently induce  
employees or users to disclose information in order to gain access to our data or  
our users' data. Although we have developed systems and processes that are  
designed to protect our data and user data, to prevent data loss, and to prevent or  
detect security breaches, we cannot assure you that such measures will provide  
absolute security.

In addition, some of our developers or other partners, such as those that help  
us measure the effectiveness of ads, may receive or store information provided by  
us or by our users through mobile or web applications integrated with Facebook.  
We provide limited information to such third parties based on the scope of services  
provided to us. However, if these third parties or developers fail to adopt or adhere



1 to adequate data security practices, or in the event of a breach of their networks,  
2 our data or our users' data may be improperly accessed, used, or disclosed.

3 Affected users or government authorities could initiate legal or regulatory  
4 actions against us in connection with any security breaches or improper disclosure  
5 of data, which could cause us to incur significant expense and liability or result in  
6 orders or consent decrees forcing us to modify our business practices. Any of these  
7 events could have a material and adverse effect on our business, reputation, or  
8 financial results.

9 29. The 1Q 2017 10-Q contained signed certifications pursuant to SOX by the Individual  
10 Defendants, stating that the information contained in the 1Q 2017 10-Q “fairly presents, in all material  
11 respects, the financial condition and results of operations of the Company for the periods presented  
12 therein.”

13 30. The statements referenced in ¶¶ 24-29 above were materially false and/or misleading  
14 because they misrepresented and/or failed to disclose the following adverse facts pertaining to the  
15 Company’s business, operational and financial results, which were known to Defendants or recklessly  
16 disregarded by them. Specifically, Defendants made false and/or misleading statements and/or failed to  
17 disclose that: (i) Facebook violated its own purported data privacy policies by allowing third parties to  
18 access the personal data of millions of Facebook users without the users’ consent; (ii) discovery of the  
19 foregoing conduct would foreseeably subject the Company to heightened regulatory scrutiny; and (iii)  
20 as a result, Facebook’s public statements were materially false and misleading at all relevant times.

21 **The Truth Begins To Emerge**

22 31. On May 16, 2017, post-market, *Reuters* published an article entitled “Facebook fined  
23 150,000 euros by French data watchdog,” reporting that the French privacy regulator CNIL had fined  
24 Facebook €150,000—the maximum amount then allowed within the CNIL’s authority—for “failing to  
25 prevent its users’ data being accessed by advertisers.” The article stated, in part:

26 Watchdog CNIL said its fine - which was imposed on both Facebook Inc and Facebook  
27 Ireland - was part of a wider European investigation also being carried out in Belgium,  
28 the Netherlands, Spain and Germany into some of Facebook’s practices.

1 The 150,000 euro fine is small in the context of the company, which has quarterly  
2 revenue of about \$8 billion and a stock market capitalization which stands at around \$435  
3 billion. But it is the maximum amount the CNIL could fine when it started the  
4 investigation on the tech giant.

5 The CNIL can now issue fines of up to 3 million euros, after the passing of a new law in  
6 October 2016.

7 \* \* \*

8 In a statement on Tuesday, Facebook did not say whether it would now take action as a  
9 result of the fine.

10 “We take note of the CNIL’s decision with which we respectfully disagree,” Facebook  
11 said in a statement emailed to Reuters.

12 32. On this news, Facebook’s share price fell \$5.34 or 3.55%, over two trading days, to  
13 close at \$144.85 on May 17, 2017.

14 33. Even after the CNIL fine, Facebook continued to conceal the extent to which its users’  
15 data was available to third parties without user consent. On July 27, 2017, Facebook filed a quarterly  
16 report on Form 10-Q with the SEC, announcing the Company’s financial and operating results for the  
17 quarter ended June 30, 2017 (the “2Q 2017 10-Q”). For the quarter, Facebook reported net income of  
18 \$3.89 billion, or \$1.32 per diluted share, on revenue of \$9.32 billion, compared to net income of \$2.27  
19 billion, or \$0.78 per diluted share, on revenue of \$6.43 billion for the same period in the prior year.

20 34. In the 2Q 2017 10-Q, the Company again offered only a non-specific representation  
21 concerning data security:

22 ***Security breaches and improper access to or disclosure of our data or user data,***  
23 ***or other hacking and phishing attacks on our systems, could harm our***  
24 ***reputation and adversely affect our business.***

25 Our industry is prone to cyber-attacks by third parties seeking unauthorized  
26 access to our data or users’ data or to disrupt our ability to provide service. Any  
27 failure to prevent or mitigate security breaches and improper access to or  
28 disclosure of our data or user data could result in the loss or misuse of such data,  
which could harm our business and reputation and diminish our competitive  
position. In addition, computer malware, viruses, social engineering  
(predominantly spear phishing attacks), and general hacking have become more  
prevalent in our industry, have occurred on our systems in the past, and will occur

1 on our systems in the future. As a result of our prominence, we believe that we are  
2 a particularly attractive target for such breaches and attacks. Such attacks may  
3 cause interruptions to the services we provide, degrade the user experience, cause  
4 users to lose confidence and trust in our products, or result in financial harm to us.  
5 Our efforts to protect our company data or the information we receive may also be  
6 unsuccessful due to software bugs or other technical malfunctions; employee,  
7 contractor, or vendor error or malfeasance; government surveillance; or other  
8 threats that evolve. In addition, third parties may attempt to fraudulently induce  
9 employees or users to disclose information in order to gain access to our data or  
10 our users' data. Although we have developed systems and processes that are  
11 designed to protect our data and user data, to prevent data loss, and to prevent or  
12 detect security breaches, we cannot assure you that such measures will provide  
13 absolute security.

14 In addition, some of our developers or other partners, such as those that help  
15 us measure the effectiveness of ads, may receive or store information provided by  
16 us or by our users through mobile or web applications integrated with Facebook.  
17 We provide limited information to such third parties based on the scope of services  
18 provided to us. However, if these third parties or developers fail to adopt or adhere  
19 to adequate data security practices, or in the event of a breach of their networks,  
20 our data or our users' data may be improperly accessed, used, or disclosed.

21 Affected users or government authorities could initiate legal or regulatory  
22 actions against us in connection with any security breaches or improper disclosure  
23 of data, which could cause us to incur significant expense and liability or result in  
24 orders or consent decrees forcing us to modify our business practices. Any of these  
25 events could have a material and adverse effect on our business, reputation, or  
26 financial results.

27 35. The 2Q 2017 10-Q contained signed certifications pursuant to SOX by the Individual  
28 Defendants, stating that the information contained in the 2Q 2017 10-Q “fairly presents, in all material  
respects, the financial condition and results of operations of the Company for the periods presented  
therein.”

36. On November 2, 2017, Facebook filed a quarterly report on Form 10-Q with the SEC,  
announcing the Company’s financial and operating results for the quarter ended September 30, 2017  
(the “3Q 2017 10-Q”). For the quarter, Facebook reported net income of \$4.70 billion, or \$1.59 per  
diluted share, on revenue of \$10.32 billion, compared to net income of \$2.62 billion, or \$0.90 per  
diluted share, on revenue of \$7.01 billion for the same period in the prior year.

1 37. The 3Q 2017 10-Q, the Company again offered only a non-specific representation with  
2 respect to data security:

3 ***Security breaches and improper access to or disclosure of our data or user data,***  
4 ***or other hacking and phishing attacks on our systems, could harm our***  
5 ***reputation and adversely affect our business.***

6 Our industry is prone to cyber-attacks by third parties seeking unauthorized  
7 access to our data or users' data or to disrupt our ability to provide service. Any  
8 failure to prevent or mitigate security breaches and improper access to or  
9 disclosure of our data or user data could result in the loss or misuse of such data,  
10 which could harm our business and reputation and diminish our competitive  
11 position. In addition, computer malware, viruses, social engineering  
12 (predominantly spear phishing attacks), and general hacking have become more  
13 prevalent in our industry, have occurred on our systems in the past, and will occur  
14 on our systems in the future. As a result of our prominence and the types and  
15 volume of personal data on our systems, we believe that we are a particularly  
16 attractive target for such breaches and attacks. Such attacks may cause  
17 interruptions to the services we provide, degrade the user experience, cause users  
18 to lose confidence and trust in our products, impair our internal systems, or result  
19 in financial harm to us. Our efforts to protect our company data or the information  
20 we receive may also be unsuccessful due to software bugs or other technical  
21 malfunctions; employee, contractor, or vendor error or malfeasance; government  
22 surveillance; or other threats that evolve. In addition, third parties may attempt to  
23 fraudulently induce employees or users to disclose information in order to gain  
24 access to our data or our users' data. Cyber-attacks continue to evolve in  
25 sophistication and volume, and inherently may be difficult to detect for long  
26 periods of time. Although we have developed systems and processes that are  
27 designed to protect our data and user data, to prevent data loss, and to prevent or  
28 detect security breaches, we cannot assure you that such measures will provide  
absolute security, and we may incur significant costs in protecting against or  
remediating cyber-attacks.

19 In addition, some of our developers or other partners, such as those that help  
20 us measure the effectiveness of ads, may receive or store information provided by  
21 us or by our users through mobile or web applications integrated with Facebook.  
22 We provide limited information to such third parties based on the scope of services  
23 provided to us. However, if these third parties or developers fail to adopt or adhere  
24 to adequate data security practices, or in the event of a breach of their networks,  
25 our data or our users' data may be improperly accessed, used, or disclosed.

26 Affected users or government authorities could initiate legal or regulatory  
27 actions against us in connection with any security breaches or improper disclosure  
28 of data, which could cause us to incur significant expense and liability or result in  
orders or consent decrees forcing us to modify our business practices. Such  
incidents may also result in a decline in our active user base or engagement levels.  
Any of these events could have a material and adverse effect on our business,  
reputation, or financial results.

1 38. The 3Q 2017 10-Q contained signed certifications pursuant to SOX by the Individual  
2 Defendants, stating that the information contained in the 3Q 2017 10-Q “fairly presents, in all material  
3 respects, the financial condition and results of operations of the Company for the periods presented  
4 therein.”

5 39. On January 31, 2018, the Company held an earnings conference call with investors and  
6 analysts to discuss the Q4 2017. During the call, Defendant Zuckerberg stated in relevant part:  
7

8 But 2017 was also a hard year. The world feels anxious and divided and that  
9 played out on Facebook. We've seen abuse on our platform, including interference  
10 from nation states, the spread of news that is false, sensational and polarizing, and  
11 debate about the utility of social media. We have a responsibility to fully  
12 understand how our services are used and to do everything we can to amplify the  
13 good and prevent the harm. This is my personal challenge for 2018.

14 \*\*\*

15 Preventing false news hate speech and other abuse[] is another important area of  
16 focus for us. In order to protect the security and integrity of our platform, we're  
17 investing in both people and technology. We now have around 14,000 people  
18 working across community ops, online ops, and our security efforts. That's almost  
19 double where we were a year-ago.

20 \*\*\*

21 Finally, we've started rolling out a major ad transparent effort. We support  
22 Congress passing legislation to make all advertising more transparent. We're not  
23 going to wait for them to act. We've already begun launching a way for anyone to  
24 view the ad, a pages running on Facebook, Instagram and Messenger, even if they  
25 aren't in the intended audience.

26 40. On February 1, 2018, Facebook filed an annual report on Form 10-K with the SEC,  
27 announcing the Company's financial and operating results for the quarter and fiscal year ended  
28 December 31, 2017 (the “2017 10-K”). For fiscal year 2017, Facebook reported net income of \$15.93  
billion, or \$5.39 per diluted share, on revenue of \$40.65 billion, compared to reported net income of  
\$10.18 billion, or \$3.49 per diluted share, on revenue of \$27.63 billion for fiscal year 2016.

41. In the 2017 10-K, with respect to the disclosure of user data, the Company again only  
offered the following non-specific representation:

***Security breaches and improper access to or disclosure of our data or user data,  
or other hacking and phishing attacks on our systems, could harm our  
reputation and adversely affect our business.***

1 Our industry is prone to cyber-attacks by third parties seeking unauthorized  
2 access to our data or users' data or to disrupt our ability to provide service. Any  
3 failure to prevent or mitigate security breaches and improper access to or  
4 disclosure of our data or user data, including personal information, content or  
5 payment information from users, could result in the loss or misuse of such data,  
6 which could harm our business and reputation and diminish our competitive  
7 position. In addition, computer malware, viruses, social engineering  
8 (predominantly spear phishing attacks), and general hacking have become more  
9 prevalent in our industry, have occurred on our systems in the past, and will occur  
10 on our systems in the future. We also regularly encounter attempts to create false  
11 or undesirable user accounts, purchase ads, or take other actions on our platform  
12 for purposes such as spamming, spreading misinformation, or other objectionable  
13 ends. As a result of our prominence, the size of our user base, and the types and  
14 volume of personal data on our systems, we believe that we are a particularly  
15 attractive target for such breaches and attacks. Such attacks may cause  
16 interruptions to the services we provide, degrade the user experience, cause users  
17 to lose confidence and trust in our products, impair our internal systems, or result  
18 in financial harm to us. Our efforts to protect our company data or the information  
19 we receive may also be unsuccessful due to software bugs or other technical  
20 malfunctions; employee, contractor, or vendor error or malfeasance; government  
21 surveillance; or other threats that evolve. In addition, third parties may attempt to  
22 fraudulently induce employees or users to disclose information in order to gain  
23 access to our data or our users' data. Cyber-attacks continue to evolve in  
24 sophistication and volume, and inherently may be difficult to detect for long  
25 periods of time. Although we have developed systems and processes that are  
26 designed to protect our data and user data, to prevent data loss, to disable  
27 undesirable accounts and activities on our platform, and to prevent or detect  
28 security breaches, we cannot assure you that such measures will provide absolute  
security, and we may incur significant costs in protecting against or remediating  
cyber-attacks.

In addition, some of our developers or other partners, such as those that help us measure the effectiveness of ads, may receive or store information provided by us or by our users through mobile or web applications integrated with Facebook. We provide limited information to such third parties based on the scope of services provided to us. However, if these third parties or developers fail to adopt or adhere to adequate data security practices, or in the event of a breach of their networks, our data or our users' data may be improperly accessed, used, or disclosed.

Affected users or government authorities could initiate legal or regulatory actions against us in connection with any security breaches or improper disclosure of data, which could cause us to incur significant expense and liability or result in orders or consent decrees forcing us to modify our business practices. Such incidents may also result in a decline in our active user base or engagement levels. Any of these events could have a material and adverse effect on our business, reputation, or financial results.

42. The 2017 10-K contained signed certifications pursuant to SOX by the Individual Defendants, stating that the information contained in the 2017 10-K "fairly presents, in all material

1 respects, the financial condition and results of operations of the Company for the periods presented  
2 therein.”

3 43. At all relevant times, Facebook has maintained a Data Use Policy on its website. At all  
4 relevant times, the Data Use Policy advised Facebook users, in part:

5 Granting us permission to use your information not only allows us to provide Facebook  
6 as it exists today, but it also allows us to provide you with innovative features and  
7 services we develop in the future that use the information we receive about you in new  
8 ways.

9 While you are allowing us to use the information we receive about you, you always own  
10 all of your information. *Your trust is important to us, which is why we don't share  
11 information we receive about you with others unless we have:*

- 12 • *received your permission;*
- 13 • *given you notice*, such as by telling you about it in this policy; or
- 14 • removed your name and any other personally identifying information from it.

15 (Emphases added) ([https://www.facebook.com/full\\_data\\_use\\_policy](https://www.facebook.com/full_data_use_policy)).

16 44. The statements referenced in ¶¶ 33-43 above were materially false and/or misleading  
17 because they misrepresented and/or failed to disclose the following adverse facts pertaining to the  
18 Company's business, operational and financial results, which were known to Defendants or recklessly  
19 disregarded by them. Specifically, Defendants made false and/or misleading statements and/or failed to  
20 disclose that: (i) Facebook continued to violate its own purported data privacy policies by permitting  
21 third parties to access the personal data of millions of Facebook users without the users' consent; (ii)  
22 discovery of the foregoing conduct would foreseeably subject the Company to heightened regulatory  
23 scrutiny; and (iii) as a result, Facebook's public statements were materially false and misleading at all  
24 relevant times.

### 25 **The Truth Begins to Emerge**

26 45. On March 17, 2018, the *New York Times* published an investigative report entitled “How  
27 Trump Consultants Exploited the Facebook Data of Millions,” revealing that Cambridge Analytica, the  
28

1 firm that worked to target voters online in connection with Donald Trump's 2016 presidential  
2 campaign, used the data of 50 million people obtained from Facebook without making proper  
3 disclosures or obtaining permission. The report further stated in relevant part:

4 *[T]he firm harvested private information from the Facebook profiles of more*  
5 *than 50 million users without their permission, according to former Cambridge*  
6 *employees, associates and documents, making it one of the largest data leaks in*  
7 *the social network's history.* The breach allowed the company to exploit the  
private social media activity of a huge swath of the American electorate,  
developing techniques that underpinned its work on President Trump's campaign  
in 2016.

8 An examination by The New York Times and The Observer of London reveals  
9 how Cambridge Analytica's drive to bring to market a potentially powerful new  
10 weapon put the firm — and wealthy conservative investors seeking to reshape  
11 politics — under scrutiny from investigators and lawmakers on both sides of the  
Atlantic.

12 \*\*\*

13 *But the full scale of the data leak involving Americans has not been previously*  
14 *disclosed — and Facebook, until now, has not acknowledged it.* Interviews with  
15 a half-dozen former employees and contractors, and a review of the firm's emails  
and documents, have revealed that Cambridge not only relied on the private  
Facebook data but still possesses most or all of the trove.

16 Cambridge paid to acquire the personal information through an outside researcher  
17 who, Facebook says, claimed to be collecting it for academic purposes.

18 During a week of inquiries from The Times, Facebook downplayed the scope of  
19 the leak and questioned whether any of the data still remained out of its control.  
But on Friday, the company posted a statement expressing alarm and promising to  
take action.

20 \*\*\*

21 In Britain, Cambridge Analytica is facing intertwined investigations by Parliament  
22 and government regulators into allegations that it performed illegal work on the  
23 "Brexit" campaign. The country has strict privacy laws, and its information  
commissioner announced on Saturday that she was looking into whether the  
Facebook data was "illegally acquired and used."

24 \*\*\*

25 The documents also raise new questions about Facebook, which is already  
26 grappling with intense criticism over the spread of Russian propaganda and fake  
27 news. The data Cambridge collected from profiles, a portion of which was viewed  
28 by The Times, included details on users' identities, friend networks and "likes."  
Only a tiny fraction of the users had agreed to release their information to a third  
party.



1 “Protecting people’s information is at the heart of everything we do,” Mr. [Paul]  
2 Grewal [Deputy General Counsel at Facebook] said. “No systems were infiltrated,  
3 and no passwords or sensitive pieces of information were stolen or hacked.”

4 Still, he added, “*it’s a serious abuse of our rules.*”

5 \*\*\*

6 Mr. Grewal, the Facebook deputy general counsel, said in a statement that both Dr.  
7 Kogan and “SCL Group and Cambridge Analytica certified to us that they  
8 destroyed the data in question.”

9 But *copies of the data still remain beyond Facebook’s control*. The Times viewed  
10 a set of raw data from the profiles Cambridge Analytica obtained.

11 (Emphases added.)

12 46. On this news, Facebook’s share price fell \$12.53, or 6.76%, to close at \$172.56 on  
13 March 19, 2018.

14 47. On March 19, 2018, post-market, *Bloomberg* published an article entitled “FTC Probing  
15 Facebook For Use of Personal Data, Source Says,” disclosing that the U.S. Federal Trade Commission  
16 is “probing whether Facebook violated terms of a 2011 consent decree of its handling of user data that  
17 was transferred to Cambridge Analytica without [user] knowledge.” Under the 2011 settlement with the  
18 FTC, Facebook “agreed to get user consent for certain changes to privacy settings as part of a  
19 settlement of federal chargers that is deceived consumers and forced them to share more personal  
20 information than they intended.” The article further stated that “if the FTC finds Facebook violated  
21 terms of the consent decree, it has the power to fine the company more than \$40,000 a day per  
22 violation.”

23 48. On March 20, 2018, several media outlets reported that the U.K. Parliament had  
24 summoned Facebook CEO Mark Zuckerberg to give evidence over the scandal involving London-based  
25 Cambridge Analytica. In a statement, the U.K. House of Commons committee on Digital, Culture,  
26 Media and Sport Committee said: “The Representatives from Facebook previously gave evidence to the  
27 inquiry in Washington DC on Thursday 8th February. However, Facebook has since failed to supply  
28

1 requested supplementary evidence to the Committee by the deadline of 14th March. Subsequent  
2 information about Facebook’s connection to Cambridge Analytica raises further questions which the  
3 Committee intends to put to Facebook to answer in full.” The British lawmakers stated they want to  
4 “hear from a senior Facebook executive with the sufficient authority to give an accurate account of this  
5 catastrophic failure of process.” Zuckerberg was asked to respond by March 26, 2018.

6  
7 49. Following these news reports, Facebook’s share price fell \$7.73, or 4.48%, to close at  
8 \$164.83 on March 20, 2018.

9 50. As a result of Defendants’ wrongful acts and omissions, and the precipitous decline in  
10 the market value of the Company’s common shares, Plaintiff and other Class members have suffered  
11 significant losses and damages.

12 **PLAINTIFF’S CLASS ACTION ALLEGATIONS**

13  
14 51. Plaintiff brings this action as a class action pursuant to Federal Rule of Civil Procedure  
15 23(a) and (b)(3) on behalf of a Class, consisting of all those who purchased or otherwise acquired  
16 Facebook common shares traded on the NASDAQ during the Class Period (the “Class”); and were  
17 damaged upon the revelation of the alleged corrective disclosures. Excluded from the Class are  
18 Defendants herein, the officers and directors of the Company, at all relevant times, members of their  
19 immediate families and their legal representatives, heirs, successors or assigns and any entity in which  
20 Defendants have or had a controlling interest.

21  
22 52. The members of the Class are so numerous that joinder of all members is impracticable.  
23 Throughout the Class Period, Facebook common shares were actively traded on the NASDAQ. While  
24 the exact number of Class members is unknown to Plaintiff at this time and can be ascertained only  
25 through appropriate discovery, Plaintiff believes that there are hundreds or thousands of members in the  
26 proposed Class. Record owners and other members of the Class may be identified from records  
27  
28

1 maintained by Facebook or its transfer agent and may be notified of the pendency of this action by mail,  
2 using the form of notice similar to that customarily used in securities class actions.

3 53. Plaintiff's claims are typical of the claims of the members of the Class as all members of  
4 the Class are similarly affected by Defendants' wrongful conduct in violation of federal law that is  
5 complained of herein.

6 54. Plaintiff will fairly and adequately protect the interests of the members of the Class and  
7 has retained counsel competent and experienced in class and securities litigation. Plaintiff has no  
8 interests antagonistic to or in conflict with those of the Class.

9 55. Common questions of law and fact exist as to all members of the Class and predominate  
10 over any questions solely affecting individual members of the Class. Among the questions of law and  
11 fact common to the Class are:  
12

- 13
- 14 • whether the federal securities laws were violated by Defendants' acts as alleged  
15 herein;
  - 16 • whether statements made by Defendants to the investing public during the Class  
17 Period misrepresented material facts about the financial condition, business,  
18 operations, and management of Facebook;
  - 19 • whether Defendants caused Facebook to issue false and misleading financial  
20 statements during the Class Period;
  - 21 • whether Defendants acted knowingly or recklessly in issuing false and  
22 misleading financial statements;
  - 23 • whether the prices of Facebook securities during the Class Period were  
24 artificially inflated because of Defendants' conduct complained of herein; and
  - 25 • whether the members of the Class have sustained damages and, if so, what is the  
26 proper measure of damages.

27 56. A class action is superior to all other available methods for the fair and efficient  
28 adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the  
damages suffered by individual Class members may be relatively small, the expense and burden of

1 individual litigation make it impossible for members of the Class to individually redress the wrongs  
2 done to them. There will be no difficulty in the management of this action as a class action.

3 57. Plaintiff will rely, in part, upon the presumption of reliance established by the fraud-on-  
4 the-market doctrine in that:

- 5 • Defendants made public misrepresentations or failed to disclose material facts  
6 during the Class Period;
- 7 • the omissions and misrepresentations were material;
- 8 • Facebook common shares are traded in efficient markets;
- 9 • the Company's shares were liquid and traded with moderate to heavy volume  
10 during the Class Period;
- 11 • the Company traded on the NASDAQ, and was covered by multiple analysts;
- 12 • the misrepresentations and omissions alleged would tend to induce a reasonable  
13 investor to misjudge the value of the Company's common shares; and
- 14 • Plaintiff and members of the Class purchased and/or sold Facebook common  
15 shares between the time the Defendants failed to disclose or misrepresented  
16 material facts and the time the true facts were disclosed, without knowledge of  
17 the omitted or misrepresented facts.

18 58. Based upon the foregoing, Plaintiff and the members of the Class are entitled to a  
19 presumption of reliance upon the integrity of the market.

20 59. Alternatively, Plaintiff and the members of the Class are entitled to the presumption of  
21 reliance established by the Supreme Court in *Affiliated Ute Citizens of the State of Utah v. United*  
22 *States*, 406 U.S. 128, 92 S. Ct. 2430 (1972), as Defendants omitted material information in their Class  
23 Period statements in violation of a duty to disclose such information, as detailed above.

24  
25 **COUNT I**

26 **Violation of Section 10(b) of The Exchange Act and Rule 10b-5**  
27 **Against All Defendants**

1           60. Plaintiff repeats and realleges each and every allegation contained above as if fully set  
2 forth herein.

3           61. This Count is asserted against Facebook and the Individual Defendants and is based  
4 upon Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), and Rule 10b-5 promulgated thereunder  
5 by the SEC.

6           62. During the Class Period, Facebook and the Individual Defendants, individually and in  
7 concert, directly or indirectly, disseminated or approved the false statements specified above, which  
8 they knew or deliberately disregarded were misleading in that they contained misrepresentations and  
9 failed to disclose material facts necessary in order to make the statements made, in light of the  
10 circumstances under which they were made, not misleading.

11           63. Facebook and the Individual Defendants violated §10(b) of the 1934 Act and Rule 10b-5  
12 in that they:  
13

- 14           • employed devices, schemes and artifices to defraud;
- 15           • made untrue statements of material facts or omitted to state material facts  
16           necessary in order to make the statements made, in light of the circumstances  
17           under which they were made, not misleading; or
- 18           • engaged in acts, practices and a course of business that operated as a fraud or  
19           deceit upon plaintiff and others similarly situated in connection with their  
20           purchases of Facebook common shares during the Class Period.

21           64. Facebook and the Individual Defendants acted with scienter in that they knew that the  
22 public documents and statements issued or disseminated in the name of Facebook were materially false  
23 and misleading; knew that such statements or documents would be issued or disseminated to the  
24 investing public; and knowingly and substantially participated, or acquiesced in the issuance or  
25 dissemination of such statements or documents as primary violations of the securities laws. These  
26 Defendants by virtue of their receipt of information reflecting the true facts of Facebook, their control  
27 over, and/or receipt and/or modification of Facebook allegedly materially misleading statements, and/or  
28

1 their associations with the Company which made them privy to confidential proprietary information  
2 concerning Facebook, participated in the fraudulent scheme alleged herein.

3 65. Individual Defendants, who are the senior officers and/or directors of the Company, had  
4 actual knowledge of the material omissions and/or the falsity of the material statements set forth above,  
5 and intended to deceive Plaintiff and the other members of the Class, or, in the alternative, acted with  
6 reckless disregard for the truth when they failed to ascertain and disclose the true facts in the statements  
7 made by them or other Facebook personnel to members of the investing public, including Plaintiff and  
8 the Class.  
9

10 66. As a result of the foregoing, the market price of Facebook common shares was  
11 artificially inflated during the Class Period. In ignorance of the falsity of Facebook's and the Individual  
12 Defendants' statements, Plaintiff and the other members of the Class relied on the statements described  
13 above and/or the integrity of the market price of Facebook common shares during the Class Period in  
14 purchasing Facebook common shares at prices that were artificially inflated as a result of Facebook's  
15 and the Individual Defendants' false and misleading statements.  
16

17 67. Had Plaintiff and the other members of the Class been aware that the market price of  
18 Facebook common shares had been artificially and falsely inflated by Facebook's and the Individual  
19 Defendants' misleading statements and by the material adverse information which Facebook's and the  
20 Individual Defendants did not disclose, they would not have purchased Facebook's common shares at  
21 the artificially inflated prices that they did, or at all.  
22

23 68. As a result of the wrongful conduct alleged herein, Plaintiff and other members of the  
24 Class have suffered damages in an amount to be established at trial.  
25

26 69. By reason of the foregoing, Facebook and the Individual Defendants have violated  
27 Section 10(b) of the 1934 Act and Rule 10b-5 promulgated thereunder and are liable to the plaintiff and  
28

1 the other members of the Class for substantial damages which they suffered in connection with their  
2 purchase of Facebook common shares during the Class Period.

3 **COUNT II**

4 **Violation of Section 20(a) of The Exchange Act**  
5 **Against The Individual Defendants**

6 70. Plaintiff repeats and realleges each and every allegation contained in the foregoing  
7 paragraphs as if fully set forth herein.

8 71. During the Class Period, the Individual Defendants participated in the operation and  
9 management of Facebook, and conducted and participated, directly and indirectly, in the conduct of  
10 Facebook's business affairs. Because of their senior positions, they knew the adverse non-public  
11 information regarding the Company's inadequate internal safeguards in data security protocols.

12 72. As officers and/or directors of a publicly owned company, the Individual Defendants had  
13 a duty to disseminate accurate and truthful information with respect to Facebook's financial condition  
14 and results of operations, and to correct promptly any public statements issued by Facebook which had  
15 become materially false or misleading.

16 73. Because of their positions of control and authority as senior officers, the Individual  
17 Defendants were able to, and did, control the contents of the various reports, press releases and public  
18 filings which Facebook disseminated in the marketplace during the Class Period. Throughout the Class  
19 Period, the Individual Defendants exercised their power and authority to cause Facebook to engage in  
20 the wrongful acts complained of herein. The Individual Defendants therefore, were "controlling  
21 persons" of Facebook within the meaning of Section 20(a) of the Exchange Act. In this capacity, they  
22 participated in the unlawful conduct alleged which artificially inflated the market price of Facebook  
23 common shares.  
24  
25  
26  
27  
28

1 74. By reason of the above conduct, the Individual Defendants are liable pursuant to Section  
2 20(a) of the Exchange Act for the violations committed by Facebook.

3 **PRAYER FOR RELIEF**

4 WHEREFORE, Plaintiff demands judgment against Defendants as follows:

5 A. Determining that the instant action may be maintained as a class action under Rule 23 of  
6 the Federal Rules of Civil Procedure, and certifying Plaintiff as the Class representative;

7 B. Requiring Defendants to pay damages sustained by Plaintiff and the Class by reason of  
8 the acts and transactions alleged herein;

9 C. Awarding Plaintiff and the other members of the Class prejudgment and post- judgment  
10 interest, as well as their reasonable attorneys' fees, expert fees and other costs; and  
11

12 D. Awarding such other and further relief as this Court may deem just and proper.  
13

14 **DEMAND FOR TRIAL BY JURY**

15 Plaintiff hereby demands a trial by jury.

16 Dated: March 20, 2018

17 Respectfully submitted,

18 **POMERANTZ LLP**

19 By: /s/ Jennifer Pafiti  
20 Jennifer Pafiti (SBN 282790)  
21 468 North Camden Drive  
22 Beverly Hills, CA 90210  
23 Telephone: (818) 532-6499  
24 E-mail: jpafiti@pomlaw.com

25 **POMERANTZ, LLP**

26 Jeremy A. Lieberman  
27 J. Alexander Hood II  
28 600 Third Avenue, 20th Floor  
New York, New York 10016  
Telephone: (212) 661-1100  
Facsimile: (212) 661-8665  
E-mail: jalieberman@pomlaw.com  
E-mail: ahood@pomlaw.com



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**POMERANTZ LLP**  
Patrick V. Dahlstrom  
Ten South La Salle Street, Suite 3505  
Chicago, Illinois 60603  
Telephone: (312) 377-1181  
Facsimile: (312) 377-1184  
E-mail: pdahlstrom@pomlaw.com

*Attorneys for Plaintiff*

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28