Kimberly C. Page (AZ # 022631)
BONNETT, FAIRBOURN, FRIEDMAN
& BALINT, P.C.
2325 E. Camelback Road, Suite 300
Phoenix, AZ 85016
Telephone:(602) 274-1100
Facsimile: (602) 274-1199
Email: kpage@bffb.com

*Liaison Counsel for the Oklahoma Police Pension and Retirement System, and the Oklahoma Firefighters Pension and Retirement System and Liaison Counsel for the Class*

*(Counsel for the Oklahoma Police Pension and Retirement System, and the Oklahoma Firefighters Pension and Retirement System and Lead Counsel for the Class Appear on the Signature Page)*

**UNITED STATES DISTRICT COURT**
**DISTRICT OF ARIZONA**

| | |
|---|---|
| Miguel Avila, on Behalf of Himself and All Others Similarly Situated,<br><br>Plaintiff,<br><br>vs.<br><br>LifeLock, Inc., Todd Davis, Chris G. Power, and Hilary A. Schneider,<br><br>Defendants. | CASE NO.: 2:15-cv-01398-SRB<br><br>**SECOND AMENDED CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

# TABLE OF CONTENTS

Lead Plaintiffs Oklahoma Police Pension and Retirement System and Oklahoma Firefighters Pension and Retirement System ("Lead Plaintiffs"), by and through their attorneys, allege the following upon information and belief, except as to those allegations concerning Lead Plaintiffs, which are alleged upon personal knowledge. Lead Plaintiffs' information and belief is based upon, among other things, their counsel's investigation, which includes without limitation: (a) review and analysis of regulatory filings made by LifeLock, Inc. ("LifeLock" or the "Company"), with the United States Securities and Exchange Commission ("SEC"); (b) review and analysis of press releases, conference calls, investor presentations, and media reports issued by and disseminated by LifeLock; (c) review of other publicly available information concerning LifeLock; (d) interviews with former employees of LifeLock ("Confidential Witnesses" or "CWs") concerning events during their tenure at the Company; (e) documents obtained from the Federal Trade Commission ("FTC") through the Freedom of Information Act ("FOIA"); (f) a declaration filed in *Ebarle v. LifeLock, Inc.*, No. 3:15-cv-00258-HSG (N.D. Cal.) (the "Ebarle Action"); and (g) consultation with Joel Winston ("Winston"), former associate director of the FTC Division of Privacy and Identity Theft Protection.

## NATURE OF THE ACTION AND OVERVIEW

1. Lead Plaintiffs bring this action on their own behalf and as a class action pursuant to Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure on behalf of a class consisting of all persons and entities who, during the period from July 30, 2014 through July 21, 2015, inclusive (the "Class Period"), purchased shares of LifeLock's publicly traded common stock and/or call options, and/or sold LifeLock's publicly traded put options, and were damaged thereby (the "Class"). Excluded from the Class are Defendants; members of the immediate families of the Individual Defendants; LifeLock's subsidiaries and affiliates, including LifeLock's employee retirement and benefit plan(s); any person who is or was an officer or director of LifeLock or any of LifeLock's subsidiaries or affiliates during the Class Period; any entity in which any Defendant has a

controlling interest; and the legal representatives, heirs, successors and assigns of any such excluded person or entity (the "Excluded Parties").

2. LifeLock provides identity theft protection services for consumers and risk management services for enterprise clients. LifeLock claims to protect its members from identity theft by monitoring identity related events, such as new account openings and credit-related applications. If LifeLock detects that a member's identity is being used, LifeLock claims that it will send its member an alert that allows the member to stop the unauthorized identity use. In the event identity theft occurs, LifeLock represents that it will assist its members in restoring their identities through the Company's remediation services. In addition, LifeLock offers The Wallet™ mobile app, which is supposed to help consumers manage their identity and payment cards on the go and enable LifeLock members to receive alerts and services on their digital devices. In short, for the price of membership, LifeLock purports to provide peace of mind for consumers amid the well-publicized threat of identity theft.

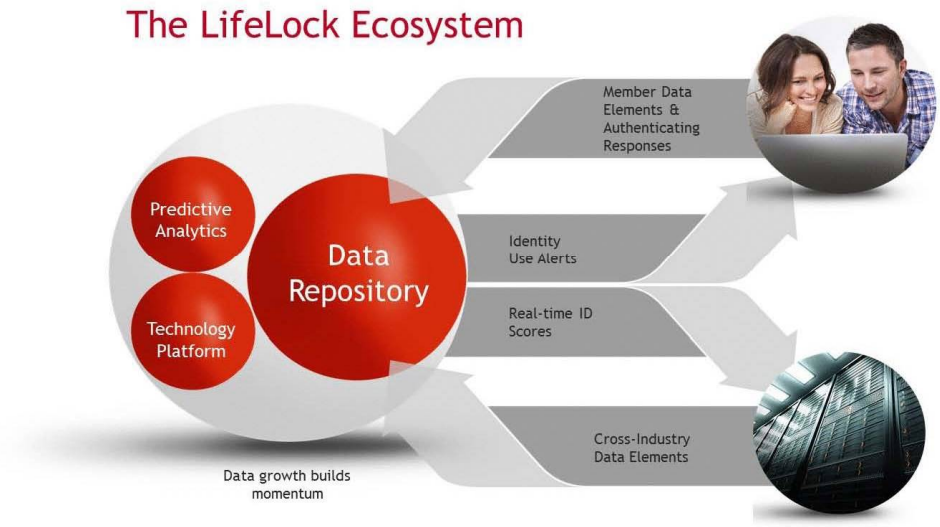
3. Since its founding in 2005, LifeLock has exploited the public's fear of data breaches and identity theft by emphasizing the myriad security risks associated with living in a digital world. In numerous filings with the SEC, LifeLock has described the cybersecurity threats that consumers face every day, from data breaches to other forms of identity theft and fraud, claiming that consumers and enterprises struggle to protect themselves effectively against these cybersecurity risks. LifeLock goes so far as to claim that: (a) the credit monitoring services most often used by consumers for identity protection are ineffective and often sell their customers' information to third parties; and (b) the self-identity risk assessments developed by some enterprises fail to provide comprehensive identity theft protection because they are often based solely on the enterprise's own records of personal information and customer transactions, and sometimes supplemented by credit reports and other third-party information.

4. To overcome these limitations, LifeLock maintains that an identity theft protection company must provide proactive and comprehensive protection against these threats. In its SEC filings and other public documents, LifeLock presents itself as the leader in providing such solutions. The foundation for these solutions is the Company's "ecosystem":

> The foundation of our identity theft protection services is the LifeLock ecosystem that combines large and constantly expanding data repositories of personally identifiable information and consumer transactions that we collect from our enterprise customers, members, and third-party fulfillment partners; proprietary predictive analytics; and a highly scalable technology platform that allows us to interact with our customers and to deliver actionable alerts to, and receive feedback from, our members and enterprise customers about potentially suspicious activity. Each day, we collect and analyze millions of data elements impacting personally identifiable information, factor in responses from our customer base to determine risk-based metrics, and enable our customers to protect against identity theft and significantly reduce the risk of identity fraud. The strength of the LifeLock ecosystem. . . . and the effectiveness of our services are enhanced with every actionable alert and transaction that we process and every new data element that we acquire.

LifeLock Inc., Annual Report (Form 10-K) (Feb. 20, 2015), at 3.

5. In its Form 10-K for the year ended December 31, 2014, LifeLock provided a graphic presentation of its "ecosystem":




6. As a result of its ecosystem (its purported combination of scale, reach, and technology), LifeLock claims that it is uniquely positioned to not only detect identity theft, but proactively prevent it from happening. Investors have taken notice of these

representations. Since October 2012, when the Company went public, the price of the Company's common stock increased two-fold, closing at $8.36 per share on October 3, 2012, and at $16.74 per share on July 14, 2015, and trading as high as $19.15 per share on December 31, 2014.

7. As alleged below, these representations, and others related to LifeLock's products and services, were materially false and misleading as verified by former employees of LifeLock, FTC documents, and a declaration submitted in a related action.

8. For example, Defendants represented that LifeLock would send its nearly 4 million members "proactive, near real-time, actionable alerts," upon detection of an identity threat. However, LifeLock's alerts did not allow its members to proactively protect their identities. Former employees of the Company and a declaration filed in the Ebarle Action both confirm that LifeLock lacked the technology and resources to provide its members with alerts in near real-time for all of the threats it was detecting. LifeLock's internal systems frequently experienced extended system shutdowns, which rendered the alert system non-functional. During these shutdowns customers did not receive alerts and thus were vulnerable to identity theft. At the same time, however, Defendants were telling the market that customers would receive an alert on a "sub-second basis" when standing in a store making a purchase. In addition, LifeLock's systems were overwhelmed by alerts and Defendants consciously decided to address the Company's inability to handle the volume of alerts by "throttling" them – that is, Defendants suppressed the issuance of alerts to certain classes of members, primarily members with poor credit ratings and the elderly.

9. In addition, a former Identity Alerts Specialist who was responsible for processing alerts and generating reports on alert trends stated that stale credit inquiry alerts went out to customers who signed up for "LifeLock Ultimate Plus" – the most comprehensive and most expensive level of LifeLock's service. According to this former employee, credit inquiry alerts were one of the main reasons for signing up for the

premium service – as these alerts would provide a notification every time a credit inquiry was made on the account (as opposed to "LifeLock Standard," the lowest and least expensive level of service, which would only provide alerts when LifeLock's proprietary algorithm detected potentially fraudulent activity). Significantly, this former employee states that ***70% of credit inquiry alerts were stale*** meaning (under the Company's own definition) that these premium customers ***would receive alerts at least a week after the threat occurred***. While touting LifeLock's services, Defendants omitted this material information from the market. Thus, in addition to shutdowns and throttling, which affected all alerts, LifeLock was sending stale alerts to over two-thirds of its highest paying customers.

10. LifeLock's Ultimate Plus package provided material amounts of revenue to LifeLock and fueled its growth. The Company launched its Ultimate Plus package at the beginning of the Class Period. Indeed, LifeLock trumpeted the increase in members and monthly average revenue per member resulting from, in part, its LifeLock Ultimate Plus services. The Company also stated that its premium service offerings, including LifeLock Advantage, LifeLock Ultimate, and LifeLock Ultimate Plus, accounted for more than 40% of its gross new members enrolled during 2014.

11. Importantly, the former Identity Alerts Specialist confirms that senior management at the highest levels of the Company, including Defendant Schneider, had access to and received regular reporting that the former Identity Alerts Specialist prepared, which showed detailed statistics on alerts that were sent out, including stale alerts. Moreover, this former employee confirmed that Defendant Schneider knew about the problems with the system regularly shutting down (during which times alerts could not be sent), the throttling, and the stale credit inquiry alerts. In particular, the former employee attended a meeting during the Class Period with Defendant Schneider where Schneider directly stated that she was aware of the stale alerts.

12. Defendants also represented that the Company maintained a comprehensive information security program that complied with the highest standards of credit protection called the Payment Card Industry Data Security Standard ("PCI DSS") that protected its members' sensitive personal data. However, former employees and FTC documents confirm that LifeLock's systems and member information was susceptible to security risks, including during system downtimes. Notably, an internal LifeLock email dated August 1, 2014, referenced in the FTC's Memorandum in Support of its Notice of Lodging Proposed Documents Under Seal stated that at the time LifeLock had "over 100 high or critical Vulnerability Remediation Requests more than 150 days old." PCI guidelines required Defendants to fix these issues monthly.

13. In addition, a few years prior to the Class Period, LifeLock was in the FTC's cross hairs for certain misrepresentations relating to its services. In or about March of 2010, the FTC filed an action in this District against LifeLock, Defendant Todd Davis, and Robert J. Maynard, Jr., a former officer of the Company, alleging, among other things, that LifeLock misrepresented the effectiveness of its identity protection services – specifically the effectiveness of its customer alerts. The FTC charged that the fraud alerts LifeLock placed on members' credit files protected against only certain forms of identity theft and gave members no protection against the misuse of existing accounts. The FTC also alleged that LifeLock provided no protection against medical identity theft or employment identity theft. The FTC further alleged that LifeLock did not, as it represented, prevent unauthorized changes to members' address information, constantly monitor activity on member credit reports, and ensure that a member would receive a telephone call from a potential creditor before a new account was opened.

14. On March 15, 2010, LifeLock entered into a decree with the FTC (the "FTC Order") pursuant to which LifeLock agreed that it would not misrepresent the "means, methods, procedures, effects, effectiveness, coverage, or scope of" any "identity theft protection . . . services," or the manner or extent to which it maintained the privacy

confidentiality, or security of personal information collected from or about members. LifeLock also agreed to establish a comprehensive data security program for the protection of members' sensitive information. Finally, the defendants agreed to pay $11 million to the FTC and $1 million to a group of 35 state attorneys general to settle the charges in the March 8, 2010 complaint.

15. Despite the injunctive provisions and prohibitions in the FTC Order, Defendants did not change the wrongful conduct underlying the FTC's complaint. Leading up to the Class Period, two high level LifeLock employees blew the whistle on Defendants' wrongful conduct, providing notice to Defendants and senior management that LifeLock was throttling and manipulating member alerts, by turning off or reducing the frequency of alerts that were to be sent to elderly customers.

16. Moreover, LifeLock's former Chief Information Security Officer averred in a legal filing that LifeLock's security posture was "high risk" and that the Company's technology security readiness and security vigilance were woefully below the minimum level necessary to protect members' sensitive personal data, again putting Defendants on notice that the Company's security system was not sufficient.

17. As alleged above, this conduct continued through the Class Period, putting LifeLock under the FTC's microscope once again. Email correspondence obtained through a FOIA request of the FTC shows that by at least January 2, 2014, and continuing through the first week of 2015, the FTC staff inquired as to whether LifeLock placed limitations on alerts to LifeLock members, and requested confirmation (which it received) that LifeLock was preserving documents because the staff intended to seek documents related to LifeLock's alert practices. At LifeLock's request, because of "the importance and immediacy of the issue," the FTC agreed to meet with LifeLock representatives on January 17, 2014. LifeLock advised the FTC staff that it wanted to use one of the whistleblower complaints as a roadmap of issues to discuss during the meeting.

18. Less than a week following the January 17, 2014 meeting, LifeLock provided documents to the FTC, including materials that were provided by the Company during the meeting. By this time, email correspondence shows that the FTC had either formally initiated an investigation, or contemplated commencing a formal investigation, of potential violations of the FTC Order. Notwithstanding, Defendants misleadingly and falsely portrayed this meeting in LifeLock's SEC filings, both before and during the Class Period, as nothing more than a discussion about the Company's "compliance" with the FTC Order in response to nuisance lawsuits.

19. The market began to learn of Defendants' fraud when on February 10, 2015, LifeLock announced that it had accrued a $20 million legal reserve for a possible settlement into LifeLock's compliance with the FTC Order, which was the decree ordering LifeLock from engaging in certain conduct, including conduct relating to the effectiveness of LifeLock's customer alerts and the effectiveness of its security system. On this news, LifeLock's stock dropped over 6% on heavy volume.

20. On July 21, 2015, the market learned the full truth when the FTC announced that it was seeking to hold LifeLock in contempt for engaging in conduct that violated the FTC Order. Among other things, the FTC alleged that LifeLock was not providing near "real-time" alerts, and not protecting members' sensitive data. On this news, the price of LifeLock's common stock plummeted, falling 49.25% to $8.15 per share after a mid-day trading halt, on unusually heavy volume.

21. As a result of Defendants' wrongful acts and omissions, and the precipitous decline in the market value of the Company's securities, Lead Plaintiffs and other Class members have suffered significant losses and damages.

## JURISDICTION AND VENUE

22. The claims asserted herein arise under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934, as amended (the "Exchange Act"), 15 U.S.C. §§ 78j(b) and 78t(a), and Rule 10b-5 promulgated thereunder by the SEC, 17 C.F.R. § 240.10b-5.

23. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331 and Section 27 of the Exchange Act, 15 U.S.C. § 78aa.

24. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) and Section 27 of the Exchange Act, 15 U.S.C. § 78aa(c). Many of the acts charged herein, including the preparation and dissemination of materially false and/or misleading information, occurred in substantial part in this District.

25. In connection with the acts, transactions, and conduct alleged herein, Defendants directly and indirectly used the means and instrumentalities of interstate commerce, including the United States mail, interstate telephone communications, and the facilities of a national securities exchange.

## PARTIES

**Lead Plaintiffs**

26. On October 9, 2015, this Court appointed the Oklahoma Police Pension and Retirement System ("Oklahoma Police") and Oklahoma Firefighters Pension and Retirement System ("Oklahoma Fire") to serve as Lead Plaintiffs in this action pursuant to the Private Securities Litigation Reform Act of 1995 (the "PSLRA") (ECF No. 31).

27. Oklahoma Police is a defined benefit pension plan that provides retirement benefits and other specified benefits to the policemen and women of Oklahoma. Oklahoma Police was established in 1981 and is based in Oklahoma City, Oklahoma. Oklahoma Police manages more than $2.2 billion in assets on behalf of more than 8,500 beneficiaries and is overseen by a 13-member board of trustees, which acts as a fiduciary for the investment of Oklahoma Police's assets. As set forth in its PSLRA certification previously filed with the Court, Oklahoma Police purchased LifeLock common stock during the Class Period and suffered damages as a result of the securities law violations alleged herein.

28. Oklahoma Firefighters is a defined benefit pension plan that provides retirement benefits and other specified benefits to Firefighters in the State of Oklahoma.

Oklahoma Firefighters was established in 1981 and is based in Oklahoma City, Oklahoma. Oklahoma Firefighters manages more than $2 billion in assets on behalf of more than 19,000 beneficiaries and is overseen by a 13-member board of trustees, which acts as a fiduciary for the investment of Oklahoma Firefighters' assets. As set forth in its PSLRA certification previously filed with the Court, Oklahoma Firefighters purchased LifeLock common stock during the Class Period and suffered damages as a result of the securities law violations alleged herein.

**Defendants**

29. Defendant LifeLock is a Delaware corporation with its principal executive offices located at 60 East Rio Salado Parkway, Suite 400, Tempe, Arizona 85281. LifeLock describes itself as a provider of proactive identity theft protection services to consumer subscribers, whom LifeLock refers to as its "members," and businesses, which LifeLock refers to as "enterprises," on an annual or monthly subscription basis. Throughout the Class Period, LifeLock common stock traded actively on the New York Stock Exchange ("NYSE") under the ticker symbol "LOCK."

30. Defendant Todd Davis ("Davis") has, at all relevant times, served as Chief Executive Officer ("CEO") of LifeLock. Davis was appointed CEO in April 2005 when the Company was founded. Davis also serves as Chairman of the Company's Board of Directors and is named as LifeLock's Principal Executive Officer in the Company's Form DEF 14A filed with the SEC on March 23, 2015. Davis is involved in the day-to-day operations of the Company and is considered to be a "key" to LifeLock's success. As noted by the Company in its SEC filings, Davis is a "key person" on which LifeLock maintains a "key person policy." According to the Company, "[t]he loss of Mr. Davis . . . could have a material adverse effect on our business." During the Class Period, as more fully alleged below, Davis made materially false and misleading statements in LifeLock's quarterly conference calls, SEC filings, industry events, and events for analysts, investors, and the media.

31. Defendant Chris G. Power ("Power") has, at all relevant times, served as Chief Financial Officer ("CFO") of LifeLock. Power was appointed CFO of LifeLock in January 2011. Power is involved in the day-to-day operations of the Company. According to CW 2, prior to and during the Class Period, Power attended and led every almost monthly Operations Review Meeting that was held for the IT, Marketing, Call Center, and Finance departments, as well as other departments within the Company. These meetings were conducted to discuss key metrics affecting the respective departments, as well as forecasting and budgeting. During the Class Period, as more fully alleged below, Power made materially false and misleading statements in LifeLock's quarterly conference calls, SEC filings, industry events, and events for analysts, investors, and the media.

32. Defendant Hilary Schneider ("Schneider") has, at all relevant times, served as President of LifeLock. She was appointed President on September 10, 2012 after spending several years as an executive at Yahoo!. In March 2016, Schneider was named Chief Executive Officer of LifeLock. According to a former Identity Alerts Specialist at LifeLock, during the Class Period, Defendant Schneider was in charge of the member services side of the business because Defendant Davis had taken a step back in order to focus more on marketing. During the Class Period, as more fully alleged below, Schneider made materially false and misleading statements during one of LifeLock's quarterly conference calls and was present and/or spoke, at a number of the conference calls, industry events, and events for analysts, investors, and the media at which Defendants Davis and Power made false and misleading statements to the market.

33. The Defendants enumerated in Paragraphs 30 through 32 are collectively referred to herein as the "Individual Defendants." The Individual Defendants together with LifeLock are referred to as the "Defendants."

34. Each of the Individual Defendants, by virtue of their high-level positions with LifeLock, directly participated in the management of the Company, was directly

involved in the day-to-day operations of the Company at the highest levels, and was privy to confidential proprietary information concerning the Company and its business, operations, growth, financial statements, and financial condition during their tenure with the Company, as alleged herein. As set forth below, the materially misstated information conveyed to the public was the result of the collective actions of these individuals. Each of these individuals, during his tenure with the Company, was involved in drafting, producing, reviewing, and/or disseminating the statements at issue in this case, approved or ratified these statements, or was aware or recklessly disregarded that these statements were being issued regarding the Company.

35. As senior executive officers and/or directors of a publicly-held company whose common stock was, and is, registered with the SEC pursuant to the Exchange Act, and whose common stock was, and is, traded on the NYSE, and governed by the federal securities laws, the Individual Defendants each had a duty to disseminate prompt, accurate, and truthful information with respect to the Company's business, operations, financial statements, and internal controls, and to correct any contemporaneous or previously issued statements that was presently or had become materially misleading or untrue, so that the market prices of the Company's publicly-traded securities would be based on accurate information. The Individual Defendants each violated these requirements and obligations during the Class Period.

36. The Individual Defendants, because of their positions of control and authority as senior executive officers and/or directors of LifeLock, were able to and did control the content of the SEC filings, press releases, and other public statements issued by LifeLock during the Class Period. Each of these individuals was provided with copies of the statements at issue in this action before they were issued to the public and had the ability to prevent their issuance or cause them to be corrected. Accordingly, each of these individuals is responsible for the accuracy of the public statements detailed herein.

37. The Individual Defendants, because of their positions of control and authority as senior executive officers and/or directors of LifeLock, had access to the adverse undisclosed information about LifeLock's business, operations, financial statements, and internal controls through access to internal corporate documents, conversations with other corporate officers and employees, attendance at LifeLock management and Board of Directors meetings and committees thereof, and via reports and other information provided to them in connection therewith, and knew or recklessly disregarded that these adverse undisclosed facts rendered the positive representations made by or about LifeLock materially false and misleading.

38. The Individual Defendants are liable as participants in a fraudulent scheme and course of conduct that operated as a fraud or deceit on purchasers of LifeLock common stock and call options and sellers of put options by disseminating materially false and misleading statements and/or concealing material adverse facts. The scheme: (i) deceived the investing public regarding LifeLock's products, business, operations, and management, and the intrinsic value of LifeLock common stock and options; and (ii) caused Lead Plaintiffs and members of the Class to acquire LifeLock common stock and/or call options at artificially inflated prices or to sell put options at deflated prices.[1]

## SUBSTANTIVE ALLEGATIONS

### A. Summary of the Claim

39. LifeLock purports to provide identity theft protection services for consumers and fraud and risk solutions for enterprises. LifeLock's threat detection, proactive identity alerts, and comprehensive remediation services purportedly provide peace of mind for consumers amid the growing threat of identity theft and identity fraud.

[1] Throughout this Complaint, references to occurrences of artificial price "inflation" also denote artificial price "deflation" in the case of put options; similarly, where the price of LifeLock's common stock and call options – or "securities" in general – is said to "decline," this also denotes that the price of put options rose, causing damage to sellers of put options. Finally, all references to "purchases" or "purchasers" of "securities" are to be read as including "sales" or "sellers" of put options.

However, as more fully set forth below, Defendants violated the federal securities laws by: (a) representing the provision of "near real-time" alerts to consumer customers as the cornerstone of LifeLock's services, when in fact, owing to lack of capacity, LifeLock intentionally ***suppressed*** and ***delayed*** such alerts to certain selected classes of customers; (b) representing that LifeLock was compliant with the very highest standards of data security protection for the personal information it acquired relating to its customers, when, in fact, LifeLock failed to take even basic steps to protect personal customer information; and (c) representing that LifeLock was in compliance with the FTC Order, and that the FTC's investigation of LifeLock's compliance was a run-of-the-mill industry-wide inquiry, when LifeLock knew that it was not in compliance with the FTC Order and that the FTC investigation was significant and likely to lead to an enforcement proceeding for contempt (as in fact it did).

40. The following background information provides context of the alleged violation of the federal securities laws.

**B. LifeLock's Products and Services**

41. LifeLock's primary method of providing identity protection to its customers is through the Company's compliment of alert services. Initially, LifeLock purchased alerts from third-party companies who had contractual permission to monitor various companies consumer transactions. LifeLock's ability to provide alerts to customers was always limited by the coverage of the third-party monitoring companies from which LifeLock received alerts; no company or combination of companies provided universal monitoring of all consumer transactions.

42. On or about March 14, 2012, LifeLock acquired one such monitoring company, ID Analytics, Inc. ("ID Analytics"), giving it direct access to ID Analytics' set of alerts along with certain patents and algorithms. The information and patents obtained from the ID Analytics acquisition allowed LifeLock to refine its monitoring system to provide alerts based on an algorithm designed to process information and detect potential

fraud. For example, during a customer transaction,[2] LifeLock reviews customers' behavioral patterns, spending patterns, velocity and location and generates a score based on the ID Analytics algorithm. If LifeLock detects a score that the Company considers sufficiently abnormal, the Company would purportedly send an alert to the customer. The customer could then respond and verify if they were the person engaging in the transaction or not. In the event that the system did not detect a score with sufficient abnormality, LifeLock would not alert the customer. This system of alerts is what LifeLock refers to as the "LifeLock Identity Alert System." The LifeLock Identity Alert System is provided to all subscribers of LifeLock, including customers subscribed to its basic, least expensive package, known as LifeLock "Standard."[3] The Standard Package retails for $9.99 a month.

43. For an additional fee, LifeLock customers can upgrade from Standard to "LifeLock Advantage" or "Ultimate Plus." Under the LifeLock Advantage subscription, LifeLock members are entitled to additional alert services such as data breach notifications and credit card, checking and savings account activity alerts. The LifeLock Advantage Plan retails for $19.99 a month. Under the Ultimate Plus subscription, the Company's most comprehensive (and most expensive) service, customers would receive all of the services provided under Basic and Advantage, as well as other alerts such as credit inquiry activity alerts, which are designed to prevent potential fraud by notifying the customer every time an inquiry about their credit-worthiness is triggered, such as during a credit card application or similar transaction. These credit inquiry activity alerts are also referred to as credit check alerts. The Ultimate Plus subscription retails for

[2] The only transactions covered by LifeLock are those which occur with LifeLock's enterprise customers or other companies LifeLock has partnered with. It is for this reason that during the Class Period LifeLock included a disclaimer on its website stating that the "Network does not cover all transactions."

[3] At the beginning of the Class Period, LifeLock introduced a new suite of identity theft services with differing levels of protection and price points known as "Standard," "Advantage" and "Ultimate Plus." These services replaced the old three-level system under which the levels were known as "LifeLock," "LifeLock Command Center" and "Ultimate."

$29.99 a month. During the Class Period, Defendants touted the Company's Ultimate Plus package as providing "the most comprehensive identity protection product in the market today."

44. During the Class Period, LifeLock had approximately 3.4 to 4 million active subscribers, of these subscribers approximately 20%, or 680,000 to 800,000, were LifeLock "Ultimate Plus" subscribers.

45. Ultimate Plus was a material portion of the Company's business, as demonstrated by both revenues and growth. For example, the November 10, 2014 Form 10-Q, signed by Defendants Power and Davis, stated as follows:

> Consumer revenue for the three-month period ended September 30, 2014 was $116.1 million, an increase of $27.7 million, or 31.4%, over consumer revenue for the three-month period ended September 30, 2013. The increase in our consumer revenue related primarily to an increase in the number of our members, which grew from 2.9 million as of September 30, 2013 to 3.5 million as of September 30, 2014, an increase of 23%. In addition, our monthly average revenue per member increased 7% to $11.22 for the three-month period ended September 30, 2014 from $10.48 for the three-month period ended September 30, 2013. **The increase in members and monthly average revenue per member resulted from the continued success of our premium service offerings, including the release of our new LifeLock Advantage and LifeLock Ultimate Plus services at the end of July 2014, and our advertising and marketing campaigns designed to increase the overall awareness of our services and identity theft.** (Emphasis added).

46. Similarly, the April 30, 2015 Form 10-Q, signed by Defendants Power and Davis, stated:

> Consumer revenue for the three-month period ended March 31, 2015 was $128.2 million, an increase of $27.2 million, or 26.9%, over consumer revenue for the three-month period ended March 31, 2014. The increase in our consumer revenue related primarily to an increase in the number of our members, which grew from approximately 3.2 million as of March 31, 2014 to approximately 3.9 million as of March 31, 2015, an increase of 21%. In addition, our monthly average revenue per member increased 5% to $11.38 for the three-month period ended March 31, 2015 from $10.81 for the three-month period ended March 31, 2014. **The increase in members and monthly average revenue per member resulted from the continued success of our premium service offerings, including the**

> **release of our new *LifeLock Advantage* and *LifeLock Ultimate Plus* services at the end of July 2014, and our advertising and marketing campaigns designed to increase the overall awareness of our services and identity theft.** (Emphasis added).

47. In addition, the Company's February 20, 2015 annual report on Form 10-K, which was also signed by Defendant Davis and Power, provided, in pertinent part:

> Consumer Services
>
> We currently offer our identity theft protection services to consumer subscribers under our LifeLock Standard, LifeLock Advantage, and LifeLock Ultimate Plus services, which we launched at the end of July 2014. We will also continue to offer our LifeLock Junior Services and, on a limited basis and for a limited time in connection with certain of our partnerships, our basic LifeLock, LifeLock Command Center, and premium LifeLock Ultimate services. We will continue to provide services to our existing members currently enrolled in our basic LifeLock, LifeLock Command Center, and premium LifeLock Ultimate services. At the heart of our consumer service offerings is our LifeLock Identity Alert system, which provides our members with notifications and alerts, including actionable alerts for new account openings and applications, and a response system for identity threats via text message, phone call, mobile application, or e-mail. **We have continued to see success with our premium service offerings, including LifeLock Advantage, LifeLock Ultimate, and LifeLock Ultimate Plus, which accounted for more than 40% of our gross new members enrolled during 2014.**
>
> * * *
>
> Revenue from our consumer segment for the year ended December 31, 2013 was $340.1 million, an increase of $85.4 million, or 33.5%, over revenue of $254.7 million for the year ended December 31, 2012. The increase in our consumer revenue from 2012 to 2013 related primarily to an increase in the number of our members, which grew from 2.5 million as of December 31, 2012 to approximately 3.0 million as of December 31, 2013, an increase of 21%. In addition, our monthly average revenue per member increased 11% to $10.32 for the year ended December 31, 2013 from $9.28 for the year ended December 31, 2012. **The increase in members and monthly average revenue per member resulted from the introduction of our LifeLock Ultimate service offering and our advertising and marketing campaigns designed to increase the overall awareness of our services and identity theft.** (Emphasis added).

**C. The FTC Order**

48. On or around 2010, the FTC conducted an investigation of LifeLock and determined that LifeLock's advertising and promotions misled consumers as to the scope and effectiveness of the identity theft protection services that LifeLock offered. The FTC also determined that there was reason to believe that LifeLock's advertising and promotions misled consumers as to the extent to which LifeLock protected the personal information that it collected from and about the consumers who purchased its services.

49. Thus, on or about March 9, 2010, the FTC commenced an action against LifeLock in this District seeking a permanent injunction and other equitable relief. *FTC v. LifeLock, Inc., et al.*, No. 2:10-cv-00530-JJT (D. Ariz. filed Mar. 9. 2010) ("FTC Complaint"). The FTC alleged that, from at least December 2006, LifeLock and its management (including Davis) "directly or indirectly . . . disseminated or caused to be disseminated to consumers advertisements and other promotional materials in connection with the advertising, promotion, marketing, offering for sale, sale, or distribution of their ID theft prevention service." FTC Complaint ¶ 17. Among such statements were the following:

- "Do you ever worry about identity theft? If so, it's time you got to know LifeLock. We work to stop identity theft before it happens. We're so confident, we back our clients with a $1 million guarantee." *Id.* ¶ 17(b).
- "We aim to stop identity theft before it happens. . . . Every three seconds an identity is stolen. We're here to make sure it doesn't happen to you." *Id.* ¶ 17(c).
- "LifeLock clients are contacted every time someone attempts to open credit in their name or change an address." *Id.* ¶ 17(g).
- "LifeLock will make your personal information useless to a criminal." *Id.* ¶ 17(i).
- "Every time you apply for new credit or someone tries to do something with your credit: You should receive a phone call from the bank asking if you are actually the person applying for credit in your name." *Id.* ¶ 17(k).
- "We work with all major credit bureaus on an ongoing basis, setting up fraud alerts and constantly monitoring what's happening with each person's credit." *Id.* ¶ 17(l).

- "LifeLock, the industry leader in proactive identity theft protection, offers a proven solution that prevents your identity from being stolen before it happens." *Id.* ¶ 17(m).

50. In fact, the FTC alleged that LifeLock's services did not live up to the promotional claims, in that LifeLock did not effectively prevent all fraudulent transactions based on misuse by others of consumers' personal information. FTC Complaint ¶18.

51. The FTC further alleged that, since at least December 2006, LifeLock and its management (including Davis) "caused to be disseminated to consumers privacy policies and statements . . . regarding the privacy, confidentiality, and security of personal information LifeLock receive from their customers." FTC Complaint ¶ 19. Among these statements were the following:

- "Only authorized employees of LifeLock will have access to the data that you provide to us, and that access is granted only on a 'need to know' basis." *Id.* ¶ 19(a).
- "Your documents, while in our care, will be treated as if they were cash." *Id.* ¶ 19(e).
- "LifeLock uses highly secure physical, electronic, and managerial procedures to safeguard the confidentiality and security of the data you provide to us." *Id.* ¶ 19(f).

52. In fact, the FTC alleged, "at least until September 2007," Defendants failed to protect personal information collected from or about consumer customers of LifeLock as they represented. FTC Complaint ¶ 20. Among other things, the FTC alleged, LifeLock and Davis:

- "Failed to limit access to personal information stored on or in transit through its networks only to employees and vendors needing access to the information to perform their jobs." *Id.* ¶ 20(c).
- "Failed, from at least December 2006 until February 2007, to secure paper documents containing personal information that were received by facsimile in an open and easily accessible area." *Id.* ¶ 20(h).

53. Less than a week after the filing of the FTC Complaint, LifeLock and Davis entered into a consent decree with the FTC dated March 15, 2010 (previously defined as

the "FTC Order"). Pursuant to the FTC Order (§ I), LifeLock and Davis were enjoined from falsely advertising the services the Company provided:

> A. in connection with the advertising, distributing, promoting, offering for sale, or sale of any product, service, or program designed for the purpose of preventing, mitigating, or recovering from any form of identity theft as defined in 18 U.S.C. § 1028, misrepresenting in any manner, expressly or by implication:
>
> > 1. that such product, service, or program provides complete protection against all forms of identity theft by making customers' personal information useless to identity thieves;
> >
> > 2. that such product, service, or program prevents unauthorized changes to customers' address information;
> >
> > 3. that such product, service, or program constantly monitors activity on each of its customers' consumer reports;
> >
> > 4. that such product, service, or program ensures that a customer will always receive a phone call from a potential creditor before a new credit account is opened in the customer's name;
> >
> > 5. the means, methods, procedures, effects, effectiveness, coverage, or scope of such product, service, or program;
> >
> > 6. the risk of identity theft to consumers;
> >
> > 7. whether a particular consumer has become or is likely to become a victim of identity theft; and/or
> >
> > 8. the opinions, beliefs, findings, or experiences of an individual or group of consumers related in any way to any such product, service, or program.
>
> Such products, services, or programs include, but are not limited to, the placement of fraud alerts on behalf of consumers, searching the internet for consumers' personal data, monitoring commercial transactions for consumers' personal data, identity theft protection for minors, and guarantees of any such products, services, or programs.
>
> B. misrepresenting in any manner, expressly or by implication, the manner or extent to which they maintain and protect the privacy, confidentiality, or security of any personal information collected from or about consumers.

54. Further pursuant to the FTC Order (§ II), LifeLock and Davis were ordered to "establish and implement, and thereafter maintain, a comprehensive information security program that is designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers":

A. the designation of an employee or employees to coordinate and be accountable for the information security program;

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to, (1) employee training and management, (2) information systems, including network and software design, information processing, storage, transmission, and disposal, and (3) prevention, detection, and response to attacks, intrusions, or other systems failure;

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, system, and procedures;

D. the development and use of reasonable steps to retain service providers capable of appropriately safeguarding personal information received from Settling Defendants and requiring service providers by contract to implement and maintain appropriate safeguards; and

E. the evaluation and adjustment of Settling Defendants' information security program in light of the results of the testing and monitoring required by Subsection C of this Section, any material changes to Settling Defendants' operations or business arrangements, or any other circumstances that Settling Defendants know or have reason to know may have a material impact on the effectiveness of their information security program.

## D. The Whistleblower Complaints

55. In the years following the issuance of the FTC Order, two former LifeLock employees filed complaints against LifeLock alleging, among other things, that LifeLock was throttling alerts to certain classes of customers by delaying or not sending them at all, despite representations to the contrary (*e.g.*, of providing proactive, near real-time alerts), in violation of the FTC Order, which enjoined Davis and LifeLock from making false representations about LifeLock's products and services. *Michael D. Peters v. LifeLock, Inc.*, No. 14-cv-00576-ROS (D. Ariz. Mar. 20, 2014) (the "Peters Compl."); *Stephen P. Burke v. LifeLock, Inc.*, No. 13-cv-01355-SPL (D. Ariz. July 8, 2013) (the "Burke Compl.").

56. In Burke's wrongful termination suit, Burke revealed that during his employment (between February 2010 and March 2013), LifeLock systemically and intentionally failed to process and send alerts to customers. According to Burke, "[t]he problem of timely informing customers that their credit information was accessed is so widespread that Defendant instituted a code freeze." As a consequence, LifeLock "deliberately 'stepp[ed] on the brakes' with regard to sending this critical information to customers on a timely basis, and worse, often choosing not to send these alerts out at all." Burke referred to the practice as "throttling." Burke Compl. ¶ 13.

57. As part of his job duties and responsibilities, "[Burke] prepared analyses on alerts provided to customers by [LifeLock]." *Id*. at ¶ 14. In the course of these responsibilities, Burke "first learned of an issue with [LifeLock's] alert notification services to customers through an e-mail chain forwarded to him in late November 2012 by John Lenstrohm ("Lenstrohm"), [LifeLock's] Director, Direct Response." *Id*. at ¶ 15.

58. Burke reported the problems related to the timing and "throttling" of alerts to the following LifeLock officers and employees, among others: Lenstrohm, Director, Direct Response; Erick Dickens, Vice President of Marketing; Amanda Mellon, Senior Manager; Brent Hazel, Manager; Melinda Keels, Finance; and Gregory Lim, Burke's immediate supervisor. Burke raised concerns about the effects of not sending out alerts, specifically that "throttling" might violate the FTC Order. *Id*. at ¶¶ 16-19. In expressing his concerns about LifeLock violating the FTC Order, Burke relied on, inter alia, the following excerpt from the Company's Form 10-K for the year ended December 31, 2012 (emphasis added):

> We protect our members by constantly monitoring identity-related events, such as new account openings and credit-related applications. If we detect that a member's personally identifiable information is being used, we offer notifications and alerts, ***including proactive, near real-time, actionable alerts*** that provide our members peace of mind that we are monitoring use of their identity and allow our members to confirm valid or unauthorized identity use.

*Id.* at ¶ 13. As alleged herein, Defendants repeated this statement in words and substance in Class Period filings with the SEC and statements to investors and market analysts.

59. In February 2014, following the FTC's renewed scrutiny of LifeLock and its violation of the FTC Order, LifeLock settled Burke's wrongful termination suit for an undisclosed amount.

60. On the heels of the Burke settlement, Peters, a LifeLock Chief Information Security Officer, corroborated Burke's allegations about throttling alerts in Peters' whistleblower complaint. In addition, Peters alleged that LifeLock provided insufficient protection for its members' private information, leaving such information unencrypted and otherwise vulnerable.

61. According to Peters, at the outset of his employment, he conducted a risk assessment of the Company's systems – a review that Peters maintained had never been conducted in earnest prior to his employment. Peters Compl. ¶ 17. The risk assessment revealed that LifeLock's technology and security were ineffective to deliver the security protections LifeLock represented in its public statements and SEC filings.

62. Specifically, Peters averred, among other things, that:

- "LifeLock's internal capacity for governance implemented (policies, audit plan, change controls, architecture review, etc.) was at 47% of the minimum to protect LifeLock's customers and their sensitive information." *Id.* at ¶ 18;
- "LifeLock's technological security readiness (intrusion prevention, data leakage, data encryption, access controls, physical security, etc.) was only at 27% of the minimum to protect LifeLock's customers and their sensitive information." *Id.* at ¶ 19; and
- "LifeLock's security vigilance (vulnerability testing, auditing, monitoring, awareness education, event logging, incident management, etc.) was at 0% of the minimum to protect LifeLock's customers and their sensitive information." *Id.* at ¶ 20.

63. According to Peters, millions of consumers were at risk, causing him to advise Defendant Power, and LifeLock Chief Information Officer, Rich Stebbins, of the

findings and the reasons therefor. In response, LifeLock fired Peters, resulting in Peters filing suit. *Id.* at ¶¶ 20-25.

64. Peters further found, among other material deficiencies, the following:

- LifeLock's director of internal audits, Tony Valentine, had collected evidence from the information security team that existed prior to Peters's arrival related to access logging, audit logging, audit log reviews, network security controls, and data leakage controls that either (1) did not truly exist because the technology was still in boxes; or (2) LifeLock lacked the staff to keep track of everything; or (3) such reviews were not actually conducted. *Id.* at ¶ 17(b).

- LifeLock employee Dave Bridgman reported that LifeLock's current practice was to manipulate the customer alerts sent to its elderly customers. LifeLock would turn off or reduce the services alerting elderly customers to reduce the call volume received by LifeLock's customer support center. *Id.* at ¶ 17(c).

- LifeLock was in the process of finalizing a new product offering called PassLock. This system was designed to allow customers to include their passwords for up to ten accounts. PassLock would then crawl through hundreds of internet sites to check the username and password supplied by the customer and report back to the customer. The problem was that the database was not being protected with industry-grade encryption. The database was predicted to contain millions of customer credentials that would be devastating to consumers if a breach occurred. Moreover, the system was going to utilize a third-party cloud hosting business without that third party's knowledge or consent. Technically, the PassLock crawling would be identified by most service providers as intrusive, illegal, illegitimate, and then blacklist the source address. *Id.* at ¶ 17(d).

65. As alleged herein, Confidential Witnesses corroborate the substantive allegations in the Burke and Peters Compls., showing that the throttled alerts and deficient security programs, procedures and protocols continued through the Class Period. Additionally, the email correspondence related to the FTC's investigation of the Company, as well as the FTC's motion to hold LifeLock in contempt for violating the FTC Order by, *inter alia*, failing: (1) to establish and maintain a comprehensive information security program to protect its users' sensitive personal data, including credit card, social security, and bank account numbers; and (2) to provide proactive, near real-time actionable alerts upon receiving an indication there was a problem with a members' information, corroborates the substantive allegations in the Burke and Peters Compls. and

the CW accounts. The allegations found in the Burke and Peters Compls. are further corroborated by excerpts from internal LifeLock emails and/or reports that describe the Company's inadequate information security systems.

**E. The FTC's Investigation of LifeLock For Violating The FTC Order**

66. On January 2, 2014, an FTC staff attorney spoke to LifeLock about the staff's concerns that LifeLock was violating the FTC Order. In particular, FTC attorney Gregory Madden ("Madden") advised counsel for LifeLock that the staff was "interest[ed] . . . [in] the 'alerts' that LifeLock provides as one of its services to its customers." Because of the FTC's interest in the "LifeLock customer alerts," Madden advised LifeLock's counsel that the FTC "may seek documents related to alerts and, in particular, limitations on alerts provided to LifeLock customers." Though not mentioning the Burke action by name, Madden referenced the Burke action and asked about a litigation hold on documents and "urge[d] LifeLock to ensure the preservation of any documents relevant to LifeLock alerts."

67. The following day, LifeLock's counsel emailed Madden to confirm the existence of a litigation hold on relevant documents and materials, and to request a meeting on January 17, 2014 to discuss the FTC's inquiry. Significantly, LifeLock's counsel advised Madden that LifeLock would "use the Burke complaint for purposes of identifying issues to discuss" at the meeting.

68. A few days later, in trying to confirm the date for the meeting, LifeLock acknowledged the "importance and immediacy of the issue" in an email to Madden.

69. By email dated January 7, 2014, Madden confirmed the meeting for January 17, 2014. Significantly, and without mentioning the Peters whistleblower complaint filed with the FTC on August 19, 2013, Madden told LifeLock that "besides [having] the discussion of 'alerts,' the FTC would also like to discuss LifeLock's information security program to protect consumers' personal information." To underscore the seriousness and scope of the inquiry, Madden requested the following:

> Specifically, we would like LifeLock to identify the employee(s) currently responsible for the company's information security program, including job titles and qualifications, and the internal organizational structure in place for reviewing and reporting on the adequacy of the information security program. In addition, we are interested in learning about internal information security risk assessments conducted since November 2012, including assessment of safeguards in place to protect consumer information, and the results of any such assessments. Please include any reviews of service providers' capabilities for protecting consumers' financial information provided to them by LifeLock. Finally, please have LifeLock identify how it receives and responds to information from third parties regarding risks to consumers' personal information.

70. The following day, LifeLock confirmed the meeting for 1:00 p.m. on January 17th at Madden's office and advised that the Company's representatives "would be prepared to address [the] list of issues (in particular, those identified in [the quote above])."

71. According to Joel Winston, former Associate Director of the FTC Division of Privacy and Identity Theft Protection, the email correspondence discussed above indicates that the FTC was contemplating opening a formal investigation into the alerts issue and the security of member information or had already done so. Email correspondence following the meeting indicates that LifeLock had been advised that the FTC was formally investigating the Company's non-compliance with the FTC Order.

72. For example, on January 22, 2014, LifeLock emailed Madden to provide materials requested by the FTC and also given to the government participants during the January 17th meeting. Significantly, LifeLock requested confidential treatment of the email and attachments – a request that, according to Winston, is often made during a formal FTC investigation. To underscore the fact that the FTC staff was contemplating and/or initiating a formal investigation, the email, as produced by the FTC pursuant to a FOIA request, has been redacted for reasons associated with a formal FTC investigation – *i.e.*, it states that it is redacted pursuant to Section 21(f) of the FTC Act, which exempts from production documents obtained by the FTC in a law enforcement investigation.

73. Emails produced pursuant to Lead Plaintiffs' FOIA request show that in the months that followed, the FTC requested documents and information from the Company,

which the Company provided. The emails also show that the FTC repeatedly sought clarification and questioned the Company's production of documents and information.

74. Attempts to resolve the undisclosed FTC staff's recommendation to file contempt proceedings for violating the FTC Order were reported in the Company's SEC filings beginning in February 10, 2015. Those attempts failed.

75. On July 21, 2015, the FTC moved to hold LifeLock in contempt for violating the FTC Order. In the notice of lodging filed in this District, the FTC identified the following underlying conduct as violative of the FTC Order:

> 1) The failure "to establish and maintain a comprehensive information security program to protect its users' sensitive personal data, including credit card, social security, and bank account numbers";
>
> 2) The failure to protect "consumers' sensitive data with the same high-level safeguards as financial institutions";
>
> 3) The failure "to meet the 2010 order's recordkeeping requirements"; and
>
> 4) "from at least January 2012 through December 2014," failing to protect "consumers' identity 24/7/365 by providing alerts 'as soon as' it received any indication there was a problem."

76. On October 28, 2015, the Company announced that it reached tentative agreements to settle lawsuits with the FTC and consumers who sued the Company for a combined $116 million.

## F. Confidential Witnesses and Consultant

77. The factual allegations below are based in part on facts provided by the following Confidential Witnesses and Consultant.

78. CW 1 was Director of Mobile Product Management at LifeLock from August 2014 to April 2015. CW 1 reported to LifeLock's Vice President of Products, Juan Paul Bedoya. As Director of Mobile Product Management, CW 1 took ownership of the Company's mobile products and applications ("apps") on both the iOS and Android platforms, and has personal knowledge about customer alerts sent through the mobile platform. CW 1 also has knowledge of the March 2015 GRANITE presentation made by LifeLock's former Director of Design and User Experience, Soudy Khan

("Khan"). CW 1 worked with Khan on a daily basis. Khan told CW 1 that he made the GRANITE presentation to LifeLock senior management.

79. CW 2 was a Senior Financial Analyst at LifeLock from June 2012 through January 2014. During the latter portion of CW 2's tenure at LifeLock, CW 2 reported to Defendant Power. Prior to that, CW 2 reported to LifeLock's Director of Finance, Gregory Lim, and LifeLock's Vice President of Finance, Audra Taylor. As a Senior Financial Analyst, CW 2 was assigned to the Company's Customer Service department, where CW 2 learned about the Company's systems and processes, including handling outgoing customer alerts and incoming customer calls. CW 2 has personal knowledge about LifeLock's inability to distribute the overwhelming amount of information received from third-party monitoring services and the Company's use of throttling to delay or suppress customer alerts. Additionally, CW 2 attended the Finance department's monthly Operating Review Meetings, which were led by Defendant Power and often attended by Defendant Davis as well as other executives. According to CW 2, customer alerts, throttling, data security issues, and system latency were frequently discussed at these meetings.

80. CW 3 was the Vice President of Marketing at LifeLock from 2007 to October 2011. CW 3 initially reported directly to Todd Davis and then to former Chief Marketing Officer, Marvin Davis after 2009. As Vice President of Marketing, CW 3 was responsible for all marketing and advertising activities at LifeLock. In this role, CW 3 developed personal knowledge of LifeLock's products, systems, and practices in order to accurately reflect the Company's service offerings in its advertisements. CW 3 has personal knowledge the Company was purposely not sending customer alerts to members who were more likely to call LifeLock, like the elderly.

81. CW 4 was employed at LifeLock from 2007 to October 2014. CW 4 began as a Member Operations Analyst and eventually transitioned into a role as a Partner Operations Implementation Specialist. From 2010 to 2012, CW 4 reported to LifeLock's

Member Operations Manager, Melissa Hanshaw. From March 2012 to May 2014, CW 4 reported to LifeLock's Manager of Member Experience and Sales Operation, Rusty Cash. From May 2014 to October 2014, CW 4 reported to LifeLock's Director of Member Services Mark Rodriguez. In CW 4's role as a Member Operations Analyst, CW 4 worked directly with ID Analytics following LifeLock's acquisition of the company, transferring ID Analytics data into LifeLock's system, and has personal knowledge about LifeLock's customer alert practices, including throttling.

82. CW 5 was an Identity Alerts Specialist at LifeLock from July 2007 to June 2015. During CW 5's tenure CW 5 reported to Anthony Aguilar, who at that time was Alert Manager and is currently Director of Member Services. In CW 5's role as an Identity Alert Specialist, CW 5 was responsible for the processing of alerts and generating reports on alert trends and sending them to Rob Ryan, Vice President of Member Services, as well as other directors within member services. According to CW 5, Ryan sent the reports to Defendant Schneider. In addition, CW 5 was responsible for managing Defendant Davis' personal LifeLock account and had power of attorney to handle issues related to his personal LifeLock account.

83. CW 6 was employed at LifeLock from July 2014 to February 2016. Initially, CW 6 started at LifeLock as Member Services Team Manager. In this role, CW 6 reported to David O'Neill, former Director of Member Services, who in turn reported to Rob Ryan, Vice President of Member Operations. In October 2015, CW 6 was promoted to Team Manager of Escalations and Identity Operations. As Team Manager of Escalations and Identity Operations, CW 6 initially reported to Rob Ryan, until Ryan was promoted. After Ryan's promotion, CW 6 reported to Eric Blomgren, former Director of Member Operations who, in turn, reported to Mike Hargis, Senior Vice President of Member Services, Consumer Sales and Business Operations, who reported to Defendant Schneider. During his tenure at LifeLock CW 6 interacted with Davis and Schneider directly. In CW 6's role as Team Manager of Escalations and Identity Operations, CW 6

dealt directly with LifeLock's customers when their complaints were elevated beyond the customer service agents and would respond on behalf of Defendant Schneider in response to their complaint letters.

84. Consultant Joel Winston is now an attorney in private practice with the firm of Hudson Cook, LLP, which he joined as a Partner in May 2012 and where he focuses his practice on consumer financial services and consumer protection matters, representing clients in government investigations, examinations, and enforcement actions before federal agencies, including the Federal Trade Commission. Prior to his time in private practice, Winston spent more than 30 years working for the FTC in a number of significant positions. From 2009 to 2011 and from 2000 to 2005, he served as the Associate Director, Division of Financial Practices. From 2005 to 2009 he was the Associate Director, Division of Privacy & Identity Protection and from 1985 to 2000 he served as Assistant Director, Division of Advertising Practices. Prior to that, he served as a staff attorney and program advisor in the FTC's offices in Washington DC. Winston's career at the FTC began in 1976, when he served as a staff attorney for four years (until 1980) in the agency's Dallas, Texas office. From 2003 to 2009, Winston served as the head of the FTC's Identity Theft Program and was responsible for starting a new FTC office tasked with protecting consumers from identity theft known as the Division of Privacy & Identity Protection. During his tenure, Winston was also the recipient of the 2008 Presidential Rank Award of Meritorious Executive and 1998 Chairman's Award, the FTC's highest award. In addition, Winston was a member of President George W. Bush's Identity Task Force, an intergovernmental group tasked with developing recommendations and solutions for identity theft. From November 11, 2011, through May 2012, Winston served as Vice President for Governmental Affairs and Chief Privacy Officer at ID Analytics, Inc. Winston left ID Analytics, Inc. prior to its consolidation with LifeLock. Prior to joining the FTC, Winston received his J.D. from the University

of Michigan Law School, Ann Arbor, Michigan, in 1976, having received a B.A. from the University of Michigan in Ann Arbor, Michigan in 1973.

## FALSE AND MISLEADING STATEMENTS

### A. LifeLock Did Not Provide Customers With Alerts That Allowed Them to Take Steps to Stop Identity Theft Transactions

#### 1. Defendants' False and Misleading Statements About "Near Real-Time" Alerts

85. Throughout the Class Period, Defendants represented to investors that the "foundation of [LifeLock's] identity theft protection services is the LifeLock ecosystem that combines large and constantly expanding data repositories of personally identifiable information and consumer transactions that [it] collect[s] from our enterprise customers, members, and third-party fulfillment partners; proprietary predictive analytics; and a highly scalable technology platform that ***allows us to interact with our customers and to deliver actionable alerts to, and receive feedback from, our members and enterprise customers about potentially suspicious activity***. . . ***The strength of the LifeLock ecosystem , . . . and the effectiveness of our services are enhanced with every actionable alert and transaction that we process and every new data element that we acquire***." *See* LifeLock Inc., Annual Report (Form 10-K) (Feb. 20, 2015) (emphasis added).[4]

86. On the first day of the Class Period, Davis described services that would be offered to customers subscribing to new categories of "Advantage" or "Ultimate Plus" service. Among these were "***data breach notifications that will keep members up to date on significant breaches, along with the recommended actions in the case of a breach***." *LOCK – Q2 2014 LifeLock Inc. Earnings Call*, Thomson Reuters Streetevents, July 30, 2014, at 3 (emphasis added). The earnings call was also attended by Defendants Power and Schneider.

[4] In the allegations of false and misleading statements, the false and misleading statements are presented in bold italics. In other parts of this Complaint, bold italics are used for emphasis.

87. On July 31, 2014, the Company filed its quarterly report for the period ending June 30, 2014 with the SEC on Form 10-Q (the "Q2 2014 10-Q"). Defendants Davis and Power signed the Q2 2014 10-Q. Relevant to the allegations in this Complaint, Defendants stated the following (emphasis added):

> ***If we detect that a member's personally identifiable information is being used, we offer notifications and alerts, including proactive, near real-time, actionable alerts that provide our members peace of mind that we are monitoring use of their identity and allow our members to confirm valid or unauthorized use.***

88. On August 5, 2014, the Company filed a Form 8-K with the SEC in which it attached a PowerPoint presentation that the Company was using in meetings to provide information about LifeLock to institutional investors and/or analysts. (The Form 8-K was filed as Exhibit 99.1 (the "LifeLock Presentation")). Slide 9 depicted the LifeLock ecosystem, and showed that one part of the system was responsible for providing "***proactive identity use alerts***" (emphasis added). Another slide (Slide 18), titled "LifeLock Consumer - 3 Layers of Protection," showed that one layer involved providing "***proactive alerts that empower customers***" (emphasis added).

89. That same day, Davis spoke at the Needham Interconnect Conference held in New York City and attended by financial analysts, investors, and members of the industry, among others. Defendant Power was also present. During the conference, Davis touted LifeLock's Ultimate Plus package as ***"clearly being the most comprehensive identity protection product in the market today."*** *LOCK - LifeLock Inc at Needham Interconnect Conference*, Thomson Reuters Streetevents, Aug. 5, 2014, at 3 (emphasis added).

90. On September 4, 2014, Davis presented at the Citi Global Technology Conference (the "Citi Conference"), a conference held in New York City and attended by financial analysts, investors, and members of the industry, among others. Accompanying Davis was Stephen Palmer, LifeLock's Controller. Davis' presentation, which was hosted by Citi analyst Jim Fish, was streamed live and hosted on the Investor Relations

page of LifeLock's website. Replays of the presentation were also made available on the Investor Relations page. During the presentation, Davis gave an example of how LifeLock provides real-time alerts to combat identity theft:

> ***[I]f you are a LifeLock subscriber, if it is you standing in that Verizon store, we will ping you, you will get it however you want to get it, email, text, whatever. You will get an alert that says, hey, we see you trying to get a new phone, is this you? And you have the chance to say yes me or no, not me. Of course, the beauty of that is if it is not you, you can stop that transaction before you become a victim of identity theft. And that applies across the board to things like new credit card applications, checking and savings accounts, payday loans, auto loans, mortgages.***

*LOCK- LifeLock Inc. at Citi Global Technology Conference*, Thomson Reuters Streetevents, Sept. 4, 2014, at 2 (emphasis added). Davis went on to assert that a positive aspect of LifeLock's acquisition of ID Analytics was that LifeLock bought "***those real-time alerts, the most valuable part of the service.***" *Id.* at 9 (emphasis added).

91. Davis similarly explained how the real-time alerts worked at the Deutsche Bank Technology Conference on September 9, 2014 (the "Deutsche Bank Conference") held in Las Vegas, Nevada. Like the Citi Conference, the Deutsche Bank Conference, which was hosted by Deutsche Bank's Nandan Amladi, was attended by financial analysts, investors, and members of the industry, among others. Accompanying Davis was Defendant Power. Davis' presentation was streamed live and hosted on the Investor Relations page of LifeLock's website. Replays of the presentation were also made available on the Investor Relations page. As he did during the Citi Conference, Davis illustrated how the real-time alerts worked:

> ***[W]e're uniquely positioned to alert one of our 3.4 million LifeLock subscribers – we see your information being used now. So even if it's you standing in the store, we can send you that real-time alert, have you see us fulfill our value proposition. You hired us to watch your back, now you see us doing that.***

*LOCK – LifeLock Inc. at Deutsche Bank Technology Conference*, Thomson Reuters Streetevents, Sept. 9, 2014, at 3 (emphasis added).

92. Following the Deutsche Bank Conference, on September 10, 2014, Deutsche Bank issued a report discussing the highlights of the first day of the conference.

In discussing LifeLock, the analysts reiterated Davis' false statements about the Company's alerts service, stating (emphasis added): "***A key differentiator is the ability to actively monitor security breaches and prevent fraudulent transactions from going through by providing real time alerts and ID scoring alerts through the capabilities acquired with the ID analytics acquisition***."

93. On November 10, 2014, the Company filed its quarterly report for the period ending September 30, 2014 with the SEC on Form 10-Q (the "Q3 2014 10-Q"). Defendants Davis and Power signed the Q3 2014 10-Q. Relevant to the allegations in this Complaint, Defendants stated the following (emphasis added):

> ***If we detect that a member's personally identifiable information is being used, we offer notifications and alerts, including proactive, near real-time, actionable alerts that provide our members peace of mind that we are monitoring use of their identity and allow our members to confirm valid or unauthorized identity use.***

94. The day after LifeLock filed the Q3 2014 10-Q, Davis and Power attended the RBC Capital Markets Technology, Internet, Media & Telecom Conference held in New York City ("RBC Capital Conference"). The RBC Capital Conference, which was hosted by RBC Capital analyst Dan Bergstrom, was attended by financial analysts, investors, and members of the industry, among others. Davis' presentation was streamed live and hosted on the Investor Relations page of LifeLock's website. Replays of the presentation were also made available on the Investor Relations page. As he did during the prior conferences, Davis illustrated how the real-time alerts worked, and explained one bad consequence the Company would suffer if real-time alerts failed:

> So we have been able to put together a network we can – for 100% of the US adult population. And so far, 3.5 million subscribers today and growing. ***We afford them the chance that, when someone goes out to open a new wireless account, get the new iPhone, when they're trying to get a new credit card, when someone wants to make a change to their checking or savings account or activity on their investment or retirement account, we actually give them a LifeLock alert. We say, . . . is this you trying to make this change, do this transaction? You have the ability to proactively say, yes, it's me or, no, it's not me. And of course if our service for any reason fails you, then we're there with a $1 million total service guarantee to say we will do the work. We're there to actually help clean it up, use our expertise, cover you on a per-incident basis up to $1 million.***

*LOCK- LifeLock Inc. at RBC Capital Markets Technology, Internet, Media & Telecom Conference*, Thomson Reuters Streetevents, Nov. 11, 2014, at 2 (emphasis added). Davis later stated, at the same conference, that LifeLock aggregates data about consumer transactions not to sell them to others, but only "***to give the most accurate, visible, real-time response back when it comes to fraud***." *Id.* at 5 (emphasis added).

95. The following day, November 12, 2014, Davis and Power presented at the Pacific Crest Internet Innovations Conference in New York City (the "Pacific Crest Conference"). The Pacific Crest Conference, which was hosted by Pacific Crest analyst Josh Beck, was attended by financial analysts, investors, and members of the industry, among others. Davis' presentation was streamed live and hosted on the Investor Relations page of LifeLock's website. Replays of the presentation were also made available on the Investor Relations page. During the presentation, Davis emphasized the importance of real-time alerts to both LifeLock's consumer customers and enterprise customers, who use LifeLock's services to monitor, in real time, the identities of consumers trying to engage in transactions with them:

> ***We are taking from our unique visibility of seeing across multiple different industries and verticals and any given moment in the most real time kind of basis to be able to say, this is – I will oversimplify, but – green status: this is Josh. You can go ahead and give them the iPhone 6. This is yellow: you should authenticate further. This is a red transaction: you probably do not want to do this. It is probably fraud.***
>
> * * *
>
> So the reason we are so effective at stopping the crime is because these criminals aren't willing to work hard or they would be productive members of society. They may be smart, but they are not willing to work real hard. The second you add friction or a spotlight to them, when they go try to monetize someone's identity, they want to get rid of it. So, if I stick with the same example, Josh, of you getting your iPhone 6***, if I am the criminal and I go in and say, hey, Verizon, I want this new iPhone. I am Josh. The second we add friction to the process, where they ping our network, they see that we are saying, hey, this one looks a little funny, we have pinged you as our client and say, Josh, is this you trying to get an iPhone? You are like, no, I am at my conference. No, not me.***
>
> ***That information then tells Verizon, do not issue this. At the time of transaction, they are going to go to the criminal and say, hey, Josh, we are going to need more identification. Our system requires that we get something else.*** The criminal[']s response is typically going to be, look, I

> don't have time for this. I'm just trying to do this on my lunch break, whatever, I'll get my iPhone; I'll come back later.
>
> ***Well, they leave. Well, they are throwing your information away because you were getting the spotlight turned on them. They are going to go out and look for easier prey. Someone that doesn't have that kind of protection.***

*LOCK – LifeLock Inc at Pacific Crest Internet Innovations Conference*, Thomson Reuters Streetevents, Nov. 12, 2014, at 2-3 (emphasis added). Davis later stated that "***what makes us materially different is that we give you that opportunity while standing in the store***." *Id.* at 4 (emphasis added).

96. On November 20, 2014, Davis presented at the Goldman Sachs US Emerging/SMID Cap Growth Conference (the "Goldman Sachs Conference"), a conference held in New York City and attended by financial analysts, investors, and members of the industry, among others. Accompanying Davis was Defendant Power. Davis's presentation, which was hosted by Goldman Sachs analyst Matt Niknam, was streamed live and hosted on the Investor Relations page of LifeLock's website. Replays of the presentation were also made available on the Investor Relations page. At the start of the presentation, Davis emphasized the "trust" that customers have in the Company because of the real-time alerts the Company purportedly sends when an intrusion is occurring:

> And we are really pleased with the idea of how many people are saying, yeah, I want LifeLock, I already trusted you. I already gave you my name, birthday, Social Security number and credit card to sign up for the service. ***Sure, I am willing to let you guys monitor the transaction, sift through them and alert me with a meaningful alert when you really see something that I should pay attention to, almost view it like the dashboard of your car.***

*LOCK- LifeLock Inc. at Goldman Sachs US Emerging/SMID Cap Growth Conference*, Thomson Reuters Streetevents, Nov. 20, 2014, at 2-3 (emphasisadded).

97. At another point, Davis gave an example of how LifeLock provides real-time alerts to combat identity theft:

> ***[S]omebody walks down the street to Verizon to get a new iPhone 6, I can immediately ping you, . . . is this you? Are you trying to get it? With one button push you can say, no, not me.***

*Id*. at 9 (emphasis added).

98. On December 4, 2014, Davis presented at the 18th Annual Credit Suisse Technology Conference (the "Credit Suisse Conference"), held in Scottsdale, Arizona and attended by financial analysts, investors, and members of the industry, among others. Accompanying Davis was Defendant Power. Davis's presentation, which was hosted by Credit Suisse analyst Michael Beresich, was streamed live and hosted on the Investor Relations page of LifeLock's website. Replays of the presentation were also made available on the Investor Relations page. At the outset of the presentation, Davis explained how the LifeLock ecosystem purportedly works, in particular the issuance of real-time alerts to prevent fraud:

> Sure. Thanks, Michael. Really we have two sides of our ecosystem, right? So there is an enterprise side where we actually – our customers are the large financial institutions, seven of the top eight. They will be the top wireless providers, so Sprint, AT&T, Verizon, Chase, HSBC, Discover Financial.
>
> So they contribute data into our data repositories about their customer information and transactions and we really [need] those -- the kind of high-value transactions. Things like when you go into a Verizon store to get the new iPhone 6 they are actually pinging our network. It's through our wholly-owned subsidiary called ID Analytics.
>
> They are pinging that network to say is Michael who he says he is? What is the risk of doing business from an identity fraud standpoint? And we are delivering in a sub-second basis an informed algorithm output, a 3 digit score that says we have taken into account everything we know about Michael and maybe even what happened minutes earlier down the street at Sprint or AT&T.
>
> * * *
>
> ***But what is really valuable is that we can also turn around and go to consumers and say if you are concerned about identity theft, we are uniquely positioned that we would send you that alert while you were in the Verizon store.***
>
> ***Or by the way, if you were up here on stage with us, Michael, you would get an alert that says, hey, are you trying to buy some new iPhones? And you could just very quickly, easily click no, not me, get back to the conference, and we have stopped identity theft. And we have sent***

> ***multifactor authentication back to Verizon to say with 100% certainty we know -- stop that transaction; it's fraud.***

*LOCK – LifeLock Inc. at Credit Suisse Technology Conference*, Thomson Reuters Streetevents, Dec. 4, 2014, at 2 (emphasis added).

99. On February 12, 2015, Davis presented at the Goldman Sachs Technology and Internet Conference 2015 (the "Goldman Sachs 2015 Conference"), held in San Francisco, California and attended by financial analysts, investors, and members of the industry, among others. Accompanying Davis were Defendants Power and Schneider. The presentation, which was hosted by Goldman Sachs analyst Matt Niknam, was streamed live and hosted on the Investor Relations page of LifeLock's website. Replays of the presentation were also made available on the Investor Relations page. During the presentation, Davis noted that LifeLock's 2012 acquisition of ID Analytics gave it exclusive access to the "***proactive alerts***" ID Analytics's technology permitted. *LOCK – LifeLock Inc. at Goldman Sachs Technology & Internet Conference*, Thomson Reuters Streetevents, Feb. 12, 2015, at 8 (emphasis added).

100. On February 20, 2015, the Company filed its annual report for the period ending December 31, 2014 with the SEC on Form 10-K (the "2014 10-K"). Defendants Davis and Power, among others, signed the 2014 10-K. Relevant to the allegations in this Complaint, Defendants stated the following:

> ***We protect our members by monitoring identity-related events, such as new account openings and credit-related applications. If we detect that a member's personally identifiable information is being used, we offer notifications and alerts, including actionable alerts for new account openings and applications, in order to provide our members peace of mind that we are monitoring use of their identity and allow our members to confirm valid or unauthorized identity use.***

2014 10-K at 46 (emphasis added).

101. On March 18, 2015, Davis presented at the Bank of America Merrill Lynch 2015 SMID Cap Conference in Boston, Massachusetts. The conference was attended by financial analysts, investors, and members of the industry, among others. Accompanying Davis was Defendant Power. The presentation was streamed live and hosted on the

Investor Relations page of LifeLock's website. Replays of the presentation were also made available on the Investor Relations page. During the presentation, Davis explained how the Company sends alerts in real time so that a customer can prevent any damage from being done to his/her identity:

> ***Are you trying to buy a new phone? We see you right now. Are you trying to get this new credit card at a Macy's or a Nordstrom? We have the ability to alert you and you the chance to do what we deem multifactor authentication.***

*LOCK – LifeLock at the BAML 2015 SMID Cap Conference*, Thomson Reuters Streetevents, Mar. 18, 2015, at 3. He later stated:

> Now we don't see every transaction in real time, but ***we're going to have the broadest coverage, give you the opportunity to say is this you trying to open this new wireless account or this new credit card account before any damage is done***.

*Id.* at 9 (emphasis added).

102. On April 30, 2015, the Company filed its quarterly report for the period ending March 31, 2015 with the SEC on Form 10-Q (the "Q1 2015 10-Q"). Defendants Davis and Power signed the Q1 2015 10-Q. Relevant to the allegations in this Complaint, Defendants stated the following (emphasis added):

> ***We protect our members by monitoring identity-related events, such as new account openings and credit-related applications. If we detect that someone is using a member's personally identifiable information, we offer notifications and alerts, including actionable alerts for new account openings and applications, in order to provide our members peace of mind that we are monitoring use of their identity and allow our members to confirm valid or unauthorized identity use.***

103. On June 3, 2015, Davis presented at the Bank of America Merrill Lynch Global Technology Conference in San Francisco, California. The conference was attended by financial analysts, investors, and members of the industry, among others. Accompanying Davis were Defendants Power and Schneider. The presentation, which was hosted by BAML analysts Kash Rangan and Scott Shiao, was streamed live and hosted on the Investor Relations page of LifeLock's website. Replays of the presentation were also made available on the Investor Relations page. As he had done in prior

conferences, Davis used the iPhone purchase to illustrate how the Company purportedly delivers near-real time alerts:

> ***LifeLock is uniquely positioned in the fact that we serve consumers, a subscription-based service, where they can come in and protect their identity where we try to send them alerts. Within our network, when we see activity, someone trying to go into get the new iPhone 6, someone trying to get a wireless account, which is something a criminal does typically right away, both because they want the devices because they can monetize those on the black market, but they also want a phone number that rings to them while they're posing as you when they open that next do, account opening.***
>
> ***We are uniquely positioned within the ecosystem that we see many of those transactions in a near real-time basis. We would be able to alert our consumers, our members that subscribe to our service and say, hey, Scott, we see you trying to get an iPhone 6.*** Hey, Kash, you're trying to open a new credit card, get a payday loan. I think things are going better with BAML. Hopefully, you don't need a payday loan. Right?
>
> ***When we see that activity we have the ability to alert you.***

*LOCK – LifeLock Inc at Bank of America Merrill Lynch Global Technology Conference*, Thomson Reuters Streetevents, June 3, 2015, at 3 (emphasis added).

104. Davis emphasized that the delivery of alerts occurs "***on a subsecond basis*** and for almost 4 million subscribers," so that customers have "***a chance to say, no, not me.***" *Id*. (emphasis added).

105. Schneider reiterated the reliability and effectiveness of real-time alerts to LifeLock's consumer customers, using the purchase of goods as an example:

> ***[T]hese alerts are very valuable to our members. We know that. If we ask you, we just detected, I'm in a Banana Republic buying something, I open a credit card, I'm standing there and I get that alert that says, your PII was just detected in a transaction. Is that you? Even if it is me and I say, yes, our users love it because they know it's working***.
>
> * * *
>
> ***I did the same thing with my son who needed something besides jeans. My son said, wow, that really works. On the alerting side, consumers really value just knowing that it doesn't take -- all you have to do is say, yes or no. It is low friction but high value to the consumer.***

*Id.* at 7-8 (emphasis added).

106. LifeLock's representations in its SEC filings and investor conferences about providing customers with real-time alerts were consistent with the representations LifeLock made on its website – a source of information investors visit in making investment decisions about a company.

107. From at least September 2014 on, LifeLock's website stated that alerts were sent "***as soon as***" potentially fraudulent transactions were detected:

> **Alerts When you Need Them**
>
> ***With our patented LifeLock Identity Alert® system, as soon as we detect a threat to your identity, you'll be notified by text, phone or email, to help stop thieves before they do damage. So while you're out there connecting to the world, we'll be here helping to keep your personal information safe.***

LifeLock, Responding to Identity Theft (Sept. 2014), https://web.archive.org/web/20140920205351/http://www.lifelock.com/how-itworks/responding/ (emphasis added).

108. Prior to August 2014, Lifelock's website boasted about how fast the response would be:

> **Taking Fast Action**
>
> ***We review each attempt to misuse your identity, and proactively contact you anytime we detect an exposure or threat. LifeLock Ultimate® protection goes one step further—if we detect a change to the contact information on your bank accounts, we'll contact you to help correct the situation fast.***

LifeLock, Responding to Identity Theft (July 2014), https://web.archive.org/web/20140718105138/http://www.lifelock.com/how-it-works/responding/ (emphasis added).

109. Other sections of the LifeLock website also included misleading information about the benefits of instant, "near real-time" alerts in stopping criminals from stealing a person's identity. For example, throughout the Class Period, a section of LifeLock's website explaining the multiple layers of protection provided by LifeLock stated, "***With the patented LifeLock Identity Alert® system, as soon as we detect a***

***threat to your identity you'll be notified by text, phone or email, to help stop criminals before they do damage to your identity***."

LifeLock, Our Services (Nov. 2014), https://web.archive.org/web/20141109114248/http://www.lifelock.com/services/ (emphasis added).

110. Indeed, throughout the Class Period, LifeLock's homepage discussed the importance of real-time alerts, stating "***When we find something suspicious, we'll let you know through our patented LifeLock Identity Alert® system.***" LifeLock, (Aug. 2014), https://web.archive.org/web/20140811185204/http://www.lifelock.com/ (emphasis added).

111. LifeLock buried meaningless and insufficient disclaimers in small-type footnotes about the alerts on its website. These footnotes, which appeared during the Class Period, stated that "[f]astest alert requires member's current email address" and "[n]etwork does not cover all transactions." LifeLock, Responding to Identity Theft (Sept. 2014), https://web.archive.org/web/20140920205351/http://www.lifelock.com/how-it-works/responding/. Nowhere did LifeLock disclose the key fact that it was throttling and/or intentionally failing to send contemporaneous alerts to certain classes of customers.

112. The securities market took account of these representations concerning the near real-time actionable alerts Defendants claimed LifeLock sends to customers. Indeed, the alerts were the subject of frequent comment by market analysts. To choose a few examples, Deutsche Bank Market Research Reports on LifeLock dated July 31, 2014, and October 30, 2014, both stated:

> Company Profile - LifeLock is a leading provider of proactive identity theft protection services for consumers and identity risk assessment and fraud protection services for enterprises. LifeLock's differentiated ecosystem combines large data repositories of personally identifiable information and consumer transactions, proprietary predictive analytics, and a highly scalable technology platform.

113. A Dougherty & Company LLC report on LifeLock dated December 5, 2014, stated:

- LifeLock, Inc. is a leading provider of proactive identity theft protection services for consumers and fraud and risk solutions for enterprises. Its threat detection, proactive identity alerts, and comprehensive remediation services help provide peace of mind for consumers amid the growing threat of identity theft. Leveraging unique data, science and patented technology from ID Analytics, Inc., a wholly-owned subsidiary, LifeLock offers identity theft protection that goes significantly beyond credit monitoring.

- LifeLock offers the most comprehensive consumer identity protection in the industry. We believe its strong brand recognition, patented and industry leading technology, and premium services differentiate it among peers. The company detects suspicious activity by constantly monitoring more than a trillion data points, uses predictive analytics to create near real time ID scores (utilized by enterprise customers), and proactivity enables consumers to respond and prevent potential threats (such as a credit card application in their name, a change to a checking account, etc.) with near real-time actionable alerts.

- LifeLock's primary alert system sends near real-time alerts to its subscribers when it detects a social security number, name, address, or date of birth in applications for credit cards, wireless services, retail credit, mortgages, auto loans, payday loans, etc. Member can choose alerts by text message, phone, or email and respond immediately to confirm if the activity is fraudulent with the company's proprietary Not Me verification technology.

114. A Dougherty & Company LLC report on LifeLock dated February 11, 2015, stated:

> Business Description: LifeLock, Inc. is a leading provider of proactive identity theft protection services for consumers and fraud and risk solutions for enterprises. LifeLock's threat detection, proactive identity alerts, and comprehensive remediation services help provide peace of mind for consumers amid the growing threat of identity theft. Leveraging unique data, science and patented technology from ID Analytics, Inc., a whollyowned subsidiary, LifeLock offers identity theft protection that goes significantly beyond credit monitoring.

115. Wright Investors' Service reports on LifeLock dated March 10, 2015, and June 11, 2015, both stated:

> It protects consumer subscribers, whom it refers to as its members, through monitoring identity-related events, such as new account openings and credit-related applications and enterprise customers through delivering on-demand identity risk and authentication information about consumers.

116. A Pacific Crest Securities report on LifeLock dated April 29, 2015, stated (emphasis added):

> LifeLock's ID Analytics and Lemon acquisitions have added technology to its platform, and ***LifeLock's ability to analyze nontraditional data from top wireless providers and credit issuers in real time and distribute alerts instantly to mobile devices puts it ahead of competitors.***

117. A Wunderlich report dated June 9, 2015, stated (emphasis added):

> Although credit bureaus including Equifax, Experian, and TransUnion provide credit event monitoring in addition to credit scoring, they are limited to their internal data that lack real-time reliability and reactivity versus proactive. ***LifeLock provides a real-time, crossindustry, deeper, and wider data sourcing of information, as well as impressive analytics, capped by a recognized brand name and unparalleled service with a guarantee.***

**2. LifeLock Did *Not* Provide "Near Real-Time" Alerts As Represented**

118. In fact, Defendants knew, or with deliberate recklessness disregarded, that LifeLock did ***not*** consistently provide "near real-time" alerts that enabled customers to proactively prevent fraudulent transactions before they were completed. As discussed herein: (a) LifeLock actively disabled alerts to specific segments of its customer population, such as customers with poor credit ratings and the elderly; (b) LifeLock delayed alerts to segments of its customer base; and (c) LifeLock had regular, weekly system downtime – often with outages of 8-12 hours – that prevented LifeLock from sending near real-time alerts. Consequently, the statements in paragraphs 85 through 110 concerning the issuance of near real-time alerts were materially false and misleading. Moreover, the statement found in paragraph 89 was additionally false and misleading because, far from providing the most comprehensive protection in the market, there was a 70% likelihood that customers enrolled in the Company's Ultimate Plus package would receive stale credit check alerts at least a week late – the most important feature of the Company's purportedly most comprehensive service.

119. In an internal presentation he made to LifeLock management in March 2015, entitle "Granite – Proposal for a more sustainable Customer Experience model," LifeLock's then-Director of Design and User Experience, Soudy Khan, described the alerts LifeLock provided customers as "stale" – they did not permit customers to proactively intervene in fraudulent transactions. In this regard, Khan wrote "that we will never best the banks and card issuers at providing alerts . . . [because it is] something we are not (and never will be) the very best at[.]"[5] Khan told CW 1 that he made this presentation to LifeLock's executives.

120. CW 5 stated that 70% of the credit check alerts were stale and that a stale alert meant that an alert was at least one week old**.** According to CW 5, the 70% chance of a week or longer delay applied to – the situation Defendant Davis described in his false and misleading statements – where a customer receives an alert while waiting in line at a Verizon store to buy a phone and having their credit check run in order to get that phone. CW 5 stated that a "huge chunk" of LifeLock's "Ultimate" customers were affected by the stale credit check alerts. CW 5 added that credit check alerts were the most common alerts as a result of there being three credit rating agencies. According to CW 5, credit check alerts were also the most important because "that's what people were paying for" by choosing the most comprehensive subscription and that there was "no value" in the credit check alerts given that there was a 70% likelihood of the alert being stale.

121. CW 5 confirmed that the highest level of management was aware of the stale alerts as well. CW 5 stated that she knew the executive team was aware of the stale alerts issue because she created reports that were sent to a "conglomerate of the executive management team." According to CW 5, the reports included detailed statistics on alerts including stale alerts and how many alerts were to be sent out. During his/her tenure, CW 5 created these reports for three types of alerts: (a) alerts from ID Analytics; (b)

[5] Should the Court so request, Plaintiffs shall submit the "GRANITE" presentation (which is labeled "confidential") *in camera* for the Court's review.

checking and savings account alerts; and (c) credit check alerts. The reports would be completed on a weekly basis and sent to LifeLock's then Alert Manager, Anthony Aguilar. According to CW 5, she would consolidate the three reports and that would be sent to executive management. CW 5 confirmed that Schneider was aware of and received this report as early as November 2014. Moreover, CW 5 confirmed that this report was sent to Defendant Schneider on a monthly basis. CW 5 knew this because Rob Ryan, Vice President of Member Services, told CW 5 that he was sending Defendant Schneider the reports and that he had meetings with Schneider about the data in the reports. CW 5 also confirmed that stale alerts were pervasive and occurred through at least June of 2015, the end of her tenure.

122. Moreover, in May 2015, CW 5, along with 15-20 others attended a luncheon with Defendant Schneider named "Have Lunch with the President Day" at LifeLock's headquarters. According to CW 5, Schneider confirmed she was aware of stale alerts issues at this luncheon while discussing "better system stability." According to CW 5, during the luncheon, one of the other attendees asked about stale alerts to which Schneider responded "I am aware of it and we are working on it."

123. Similarly, CW 6, who confirmed that the stale alerts continued even after the Class Period, also stated that a lot of problems including stale alerts were elevated to LifeLocks's executive management but that they tended to fall on "deaf ears" even though CW 6 would hear about stale alerts "all the time . . . constantly." CW 6 also attributed the stale alerts to "issues in [Lifelock's] systems."

124. Confidential Witnesses also explained that LifeLock's ecosystem was unable to provide the comprehensive protection against identity theft and identity fraud that the Company represented it would to investors and the public. These CWs describe a system that was plagued by inadequate technology and staffing, which prevented the Company from sending near real-time alerts and prevented LifeLock customers from being able to proactively respond to identity theft and identity fraud threats.

125. CW 2 explained that LifeLock used third-party vendors to provide the information underlying the alerts that LifeLock would send to its customers. According to CW 2, the amount of information that was coming into LifeLock during the CW's witness's tenure (from June 2012 through January 2014) was overwhelming. LifeLock did not have processes in place to distribute that information. After obtaining and processing the information from the monitoring services, LifeLock sent the alerts to its customers. In response, call volume would "blow up." However, LifeLock did not have enough agents to handle follow-ups from all of the alerts.

126. Rather than improving its technology and staffing to enable the Company to provide the services it represented, LifeLock purposely delayed or suppressed alerts, without advising customers – or investors – that it was doing so. More particularly, both prior to and during the Class Period, LifeLock engaged in the practice known as "throttling," whereby it purposely delayed or suppressed alerts to certain classes of its customers. As CW 3 explained, during times when LifeLock's call centers were lightly staffed, LifeLock would suppress alerts to elderly customers, because those customers were the more likely to burden LifeLock with calls. As whistleblower Peters alleged:

> LifeLock employee Dave Bridgman told Peters that LifeLock's current practice was to manipulate the customer alerts sent to its elderly customers. LifeLock would turn off or reduce the services alerting elderly customers to reduce the call volume received by LifeLock's customer support center.

Peters Compl. ¶ 17(c). CW 4 added that during the Class Period, LifeLock similarly "throttled" alerts to customers with lower credit ratings, on the theory that those customers had the least to lose from failing to receive alerts as their credit ratings were impaired already.

127. CW 4 stated that, toward the end of the witness's tenure in October 2014, LifeLock would only send out a total of about 1,000 alerts per weekday – even though LifeLock received as many as 5,000 potential fraud or identity theft alerts per weekday.

128. According to CW 4, LifeLock took its computer system offline for maintenance every Tuesday and Thursday night, for as much as 12 hours each time and

that these shutdowns continued until the end of her tenure at LifeLock. During these twice-weekly down periods, new alerts could not be sent out, and customer service personnel could not respond to customer inquiries regarding alerts previously sent.

129. CW 5 likewise confirmed that throughout the Class Period, LifeLock's systems would go down regularly. CW 5 explained that when the systems went down some members would not get alerts and when the systems started back up there would be a push to get all of the alerts out and "some fell through the cracks for sure." CW 5 also stated in 2014 and 2015 it was a "constant roller coaster with the systems" and that system outages occurred during the day as well as overnight.

130. Moreover, CW 5 confirmed that Schneider was also aware of system shutdown issues and the throttling of the Early Warning System alerts because those issues were also discussed by Schneider during the "Have Lunch with the President Day" meeting. According to CW 5, during the luncheon, Schneider explained to the attendees that she was "working with the IT people" including the CIO and CTO to get "better system stability."

## B. LifeLock Did Not Provide Its Customer's Personal Information Sufficient Security Protection – Much Less the Very Highest Level, as Defendants Represented

### 1. LifeLock's False and Misleading Statements About Customer Data Security

131. Throughout the Class Period, Defendants represented that LifeLock complied with the highest standards of data security applicable to major financial institutions, which is known as Level 1 of the Payment Card Industry Data Security Standard ("PCI DSS"). PCI DSS is a set of requirements, formulated by an industry group in the payment card industry, designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. The highest level of data security under this industry standard, used by large banks and other financial institutions, is Level 1.

132. At the Deutsche Bank Technology Conference on September 9, 2014, Deutsche Bank Analyst Nandan Amladi asked Davis how LifeLock protected the highly confidential data that customers provided to the Company. Davis replied that "[f]rom the day [he] founded the Company," he knew that LifeLock was "consolidating all the keys to the kingdom, as we call it – name, birth date, Social Security Number, plus now checking and savings accounts, credit card numbers, account information." *LOCK-LifeLock Inc. at Deutsche Bank Technology Conference*, Thomson Reuters Streetevents, Sept. 9, 2014, at 4. Since data handling and information security were of paramount importance to LifeLock's ecosystem, Davis explained that the Company had to operate under the PCI Level 1 security standard:

> ***So of course we're going to look to operate under the highest data handling and data security standards, PCI Level 1, for our core business, right? That's how we're going to make sure that we operate . . . .***

*Id.* (emphasis added).

133. Davis' statement about operating under the PCI Level 1 security standard was explained in more detail on LifeLock's website. Indeed, at all times throughout the Class Period, LifeLock's website contained a discussion in which the Company represented that its security credentials included "PCI level 1" compliance (emphasis added):

> **Our Credentials**
>
> At LifeLock, relentless protection of your identity is our primary mission. Here are just a few examples of the steps we take to help ensure you stay ahead of identity thieves:
>
> First in the industry to offer proactive identity theft protection
>
> ***Level 1 compliant under the Payment Card Industry Data Security Standard***
>
> Member of TRUSTe
>
> Direct access to fraud resolution teams within our extensive network of lenders and service providers
>
> Expert thought leadership with internationally recognized experts in privacy and security technologies, fraud, and criminal methods

Partnerships with FBI Law Enforcement Executive Development Association (FBI-LEEDA), National Organization for Victim Assistance (NOVA).

**2. LifeLock Was Not PCI DSS Level 1 Compliant, and Did Not Provide Adequate Data Security Protection for Its Customers' Personal Information**

134. In fact, Defendants knew, or with deliberate recklessness disregarded, that LifeLock did not provide the level of data security protection for its customers' personal information that Defendants claimed. As set forth in the Peters Compl. and confirmed by Confidential Witnesses, LifeLock failed to:

(a) encrypt personal customer information, but rather stored and transmitted it in readable text;
(b) limit access to personal customer information to those LifeLock employees and contractors who needed such access for the performance of their jobs;
(c) install critical patches and updates to avoid known security threats; and
(d) comply with PCI DSS Level 1 requirements at all relevant times.

135. Peters – LifeLock's former Chief Information Security Officer – alleged facts in his whistleblower complaint that demonstrate LifeLock's failure to provide personal customer data with adequate security protection. Peters averred that:

- LifeLock's technological security readiness was only 27% of the minimum needed to protect the personal information of LifeLock's customers,
- LifeLock's security vigilance was 0% of the minimum needed to protect the information of LifeLock's customers, and
- LifeLock's internal capacity for implementing governance regarding security was only 47% of the minimum needed to protect the personal information of LifeLock's customers.

Peters Compl. ¶¶ 18-20.

136. Peters alleged that one of the principal causes of LifeLock's inadequate data security protection was insufficient staffing, and that he asked to immediately hire an additional 12 information security professionals to bring LifeLock up to even the minimum level necessary for information security – but LifeLock's management

responded that the Company would hire no more than two additional security professionals (if that many) within the next year, and that full staffing would take years to reach, if it was to be done at all. Peters Compl. ¶ 22.

137. Peters alleged that he discussed his concerns about LifeLock's inadequate customer data security protection directly with Defendant Power on or about July 9, 2013.

138. Emails produced pursuant to Lead Plaintiffs' FOIA request show that the FTC staff was taking Peters' allegations seriously. On January 7, 2014, Madden informed LifeLock that, in addition to alerts, the FTC staff "would also like to discuss LifeLock's information security program to protect consumers' personal information," during the meeting on January 17, 2014. Madden requested the following:

> Specifically, we would like LifeLock to identify the employee(s) currently responsible for the company's information security program, including job titles and qualifications, and the internal organizational structure in place for reviewing and reporting on the adequacy of the information security program. In addition, we are interested in learning about internal information security risk assessments conducted since November 2012, including assessment of safeguards in place to protect consumer information, and the results of any such assessments. Please include any reviews of service providers' capabilities for protecting consumers' financial information provided to them by LifeLock. Finally, please have LifeLock identify how it receives and responds to information from third parties regarding risks to consumers' personal information.

139. The FTC's information request mirrors the areas of LifeLock's information security program identified as insufficient in the Peters Compl.

140. Additionally, LifeLock's information security program was woefully inadequate to protect customer information and was out of compliance with PCI DSS v3.0.[6]

[6] Version 3.0 of the Payment Card Industry Data Security Standard was published in November 2013 and was the operative PCI DSS standard at the time Defendants made false and misleading statements to the market about the Lifelock's compliance with PCI Level 1 standards. *See* PCI Sec. Standards Council, Payment Card Industry (PCI) Data Security Standard, v3.0 (Nov. 2013), https://www.pcisecuritystandards.org/document_library.

141. PCI DSS Requirement 6.1 of PCI DSS v3.0 required LifeLock to "[e]stablish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as 'high,' 'medium,' or 'low') to newly discovered security vulnerabilities." PCI DSS v3.0, at 49. In addition, Requirement 6.1 notes:

> Risk rankings should, at a minimum, identify all vulnerabilities considered to be a 'high risk' to the environment. In addition to the risk ranking, vulnerabilities may be considered 'critical' if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.

*Id*.

142. PCI DSS Requirement 6.2 required LifeLock to "[e]nsure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. *Id*. at 50. And to "[i]nstall critical security patches within one month of release." *Id*. PCI DSS Requirement 6.2 goes on to note: "Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1." *Id*.

143. Security patches are typically available within one month of a vulnerability being identified. For example, Microsoft has released security patches on the second Tuesday of every month. *See Microsoft Security Bulletins*, MICROSOFT SECURITY TECHCENTER, https://technet.microsoft.com/en-us/security/bulletins.aspx (last visited Sept. 22, 2015) (stating Microsoft security updates are released on the second Tuesday of each month). For more critical vulnerabilities, patches are often released even faster.

144. Internal LifeLock emails cited in the FTC's Memorandum in Support of its Notice of Lodging Proposed Documents Under Seal, obtained through a FOIA request, confirm that LifeLock's internal systems were out of compliance with the applicable PCI DSS v3.0 requirements during the Class Period. Specifically, the FTC's Memorandum

confirms that "LifeLock failed to timely remediate many known critical system vulnerabilities." For example, one internal LifeLock email dated August 1, 2014, referenced in the FTC's Memorandum in Support of its Notice of Lodging Proposed Documents Under Seal, stated that there were "over 100 high or critical Vulnerability Remediation Requests more than 150 days old." These high or critical vulnerabilities went unaddressed more than five times longer than allowed under PCI DSS v3.0 Requirements 6.1 and 6.2.

145. CWs also confirm what is contained in the LifeLock emails referenced by the FTC – namely, that prior to and during the Class Period, LifeLock's data security program did not adequately protect customers' personal information. CW 3 said that LifeLock had data protection issues and the Company purported to be PCI Level 1 compliant, but was not. Similarly, CW 2 also asserted that third parties call centers contracted by LifeLock were not PCI Level 1 compliant and had no intention of becoming so at any reasonable pace.

146. CW 4 stated that senior management at LifeLock told LifeLock employees, including the witness, that it would cost as much as $100 million to bring LifeLock into compliance, but that the Company did not intend to spend that money. In addition, in a meeting in or about March or April 2013, CW 4 communicated concerns about LifeLock's data security protection to Defendant Hilary Schneider, and Schneider replied that the Company had other priorities. During the conversation CW 4 explained to Schneider that LifeLock needed to update their systems because their system could not handle large enrollments or automation and required frequent system shutdowns. Moreover, CW 4 told Defendant Schneider that the system issues made enrollment more difficult and affected LifeLock's members directly. Schneider responded to CW 4 that in order to fix the problem, it would take a $100 million system overhaul and LifeLock "can't afford that."

147. CW 4 referred to a conspiracy within the Company to cover up its lack of PCI compliance. Among other things, in or about January or February 2014, LifeLock Director of Internal Audits Tony Valentine instructed the witness not to communicate any facts concerning LifeLock's data security problems to auditors.

148. Aside from its lack of PCI compliance, LifeLock failed to take the most basic steps to protect its customers' personal information. CW 4 reported that when LifeLock made product demonstrations to potential "partners" – companies that would retain LifeLock to provide data protection services to employees – the partners' representatives would be allowed to watch LifeLock's employees operate the computers accessing consumer customers' information, where they were able to see screens containing personal customer information.

149. CW 4 also reported that customer information was vulnerable during the twice-weekly extended shutdowns of LifeLock's computer systems. *See* ¶ 128. Additionally, according to a declaration filed in the Ebarle Action, from January 1, 2012 to April 30, 2015 LifeLock was unable to provide alerts during multiple planned and unplanned system outages and could not provide certain alerts during 42 different weekends during that time.

150. Moreover, according to CW 4, LifeLock did not always encrypt customer information properly (or at all), thus rendering that information vulnerable to breaches.

### C. Defendants Misled Investors by Misrepresenting the Severity of the FTC's Investigation of LifeLock

151. Throughout the Class Period, LifeLock represented to investors that the FTC's inquiries into its customer alerts and data security protection of customer information were nothing more than a run-of-the-mill inquiry, initiated at LifeLock's insistence in response to a cash-grabbing whistleblower, that was part of the FTC's routine monitoring of the consumer data protection industry as a whole. In fact, Defendants were aware, as early as January 2, 2014, that LifeLock was being specifically targeted by the FTC for an investigation into matters as to which it was non-compliant

with the FTC Order – and, as early as February 4, 2015, when LifeLock made a $20 million settlement offer to the FTC, that an enforcement action (in the form of a motion to hold LifeLock in contempt) was imminent and that the action was likely to result in significant penalties.

152. Prior to the beginning of the Class Period, Defendants spoke about the Company's interactions with the FTC, which formed the foundation for the Class Period misstatements about the FTC's scrutiny of the Company and its violation of the FTC Order.

153. On February 19, 2014, LifeLock filed its Form 10-K for the year ending December 31, 2013 (the "2013 Form 10-K"). In the 2013 Form 10-K, Defendants downplayed the scope and severity of the FTC investigation and attributed the FTC's inquiry to routine industry wide scrutiny and a cash-grabbing whistleblower, stating:

> ***With the growing public concern regarding privacy and the collection, distribution, and use of consumer personal information, we believe we are in an environment in which there is an increased regulatory scrutiny concerning data collection and use practices and the provision and marketing of services, like ours, that seek to protect that information. We expect that kind of scrutiny to continue as the marketplace for services like ours continues to develop. In addition, we believe there has been a recent increase in whistleblower claims made to regulatory agencies, including whistleblower claims made by former employees, which we believe will likely continue, in part because of the provisions enacted by the Dodd-Frank Wall Street Reform and Consumer Protection Act, or the Dodd-Frank Act, that may entitle persons who report alleged wrongdoing to the SEC to cash rewards. Often, the allegations underlying such claims to regulatory agencies result in federal and state inquiries and investigations. On January 17, 2014, we met with FTC Staff, at our request, to discuss issues regarding allegations that have been asserted in a whistleblower claim against us relating to our compliance with the FTC Order. Following this meeting, we expect to receive either a formal or informal investigatory request from the FTC for documents and information regarding our policies, procedures, and practices for our services and business activities. Given the heightened public awareness of data breaches and well as attention to identity theft protection services like ours, it is also possible that the FTC, at any time, may commence an unrelated inquiry or investigation of our business practices and our compliance with the FTC Order. We endeavor to comply with all applicable laws and believe we are in compliance with the requirements of the FTC Order. We believe the increased regulatory scrutiny will continue in our industry for the foreseeable future and could lead to additional meetings or inquiries or investigations by the agencies that regulate our business, including the FTC.***

2013 Form 10-K at 10 (emphasis added).

154. In Class Period filings and conferences, Defendants used various forms of the quoted language in paragraph 153 above, to convey a false and misleading impression that the Company was compliant with the FTC Order – LifeLock initiated contact with the FTC proactively to discuss its compliance, as opposed to non-compliance, with the FTC Order – and that the FTC was only making inquiries of the Company, as opposed to formally investigating the Company for violating the FTC Order.

155. On March 17, 2014 the Company first made mention of the FTC inquiry when it filed a Form 8-K, stating "[o]n March 13, 2014, LifeLock received, as expected, a request from the FTC for documents and information related to LifeLock's compliance with the FTC Stipulated Final Judgment and Order for Permanent Injunction and Other Equitable Relief that LifeLock entered into in March 2010."

156. On July 31, 2014, the Company filed its quarterly report for the period ending June 30, 2014 with the SEC on Form 10-Q (the "Q2 2014 10-Q"). Defendants Davis and Power signed the Q2 2014 10-Q. Defendants stated the following (emphasis added):

> ***On March 13, 2014, we received a request from the Federal Trade Commission, or the FTC, for documents and information related to our compliance with the FTC Order. Prior to our receipt of the FTC's request, we met with FTC Staff on January 17, 2014, at our request, to discuss issues regarding allegations that have been asserted in a whistleblower claim against us relating to our compliance with the FTC Order. On March 13, 2014, we received a request from the FTC for documents and information related to our compliance with the FTC Order. We are in the process of completing our response to the FTC's March 13, 2014 request for information regarding our information security program and alert and notification processing, along with a subsequent request for clarification regarding certain information that we previously submitted.***

157. On August 5, 2014, Davis presented at the Needham Interconnect Conference held in New York City and attended by financial analysts, investors, and members of the industry, among others. Accompanying Davis was Defendant Power. Davis' presentation, which was hosted by Needham analyst Scott Zeller, was streamed

live and hosted on the Investor Relations page of LifeLock's website. Replays of the presentation were also made available on the Investor Relations page. The presentation was conducted in the form of questions and answers between Zeller, on the one hand, and Davis and Power, on the other hand. In one exchange, Zeller asked Davis about the Company's "dialog" with the FTC. In response, Davis dismissively characterized Burke and Peters as disgruntled employees and/or untrustworthy individuals who did not blow the whistle on the Company:

> ***So kind of reminding people, initially there were a couple of different whistleblower claims that were brought by former employees. The first one that was brought we were able to resolve fairly quickly favorable to the company and that individual double-tracked their previous claims. The other one is ongoing with a former employee who was with us for less than 30 days. Not granted in the seesaw rule, but because of the fact that we found that there was deception in resumes and application, we didn't want to have the person in charge of information security. Someone that we found was not being honest at the time they applied for the jobs. So it was terminated for those reasons, having to nothing to do with whistleblower. But we wanted to in kind of an unusual situation, we actually proactively ask for a meeting with the FTC to try to address things, straightforward head up.***

*LOCK- LifeLock Inc. at Needham Interconnect Conference*, Thomson Reuters Streetevents, Aug. 5, 2014, at 5 (emphasis added).

158. In the earnings call with investors and market analysts on October 29, 2014, Davis falsely implied that the FTC was merely conducting an inquiry in which it was engaged an "initial data and question gathering process":

> ***[W]e are continuing to cooperate with the FTC as they work through their process. At this point, we have answered all of the questions they have posed to us. We could certainly receive more questions before this process is complete, but I wanted to provide a status update as to where we stand today. Even if we, indeed, are at the end of the initial data and question gathering process, there is still no way for me to predict when the FTC's inquiry may be completed.***

*LOCK – Q3 2014 LifeLock Inc. Earnings Call*, Thomson Reuters Streetevents, Oct. 29, 2014, at 4 (emphasis added).

159. On November 10, 2014, the Company filed its quarterly report for the period ending September 30, 2014 with the SEC on Form 10-Q (the "Q3 2014 10-Q").

Defendants Davis and Power signed the Q3 2014 10-Q. Relevant to the allegations in this Complaint, Defendants stated the following (emphasis added):

> On March 13, 2014, we received a request from the FTC for documents and information related to our compliance with the FTC Order. Prior to our receipt of the FTC's request, we met with FTC Staff on January 17, 2014, at our request, to discuss issues regarding allegations that have been asserted in a whistleblower claim against us relating to our compliance with the FTC Order. On October 29, 2014, we completed our responses to the FTC's March 13, 2014 request for information along with the FTC's subsequent requests for clarification regarding certain information that we previously submitted. ***The FTC may request additional information or clarification on the information submitted or may request that we discuss with the FTC the issues relating thereto.***

160. At the RBC Conference on November 11, 2014, Davis falsely stated that the Company was complying with the FTC in discussing how such compliance served as an "overhang" on operations:

> ***I think from our perspective we believe there is this overhang from FTC inquiries into us as we operate under an FTC consent decree. That being said, we're working as aggressively as we can. We have provided all of the responses to the FTC today. And as of today, and with the last earnings call, we have what's called certified our responses. So that is meaning that we have documented signoff on we've responded to everything now.*** To be clear . . . that doesn't meant they can't come back and decide they want to ask some more questions or get some more data. ***But at this point, today, we are in a position that we've delivered everything to them and now, from our perspective, we have to wait and it's kind of in their court from there.***

*LOCK – LifeLock Inc. at RBC Capital Markets Technology, Internet, Media & Telecom Conference*, Thomson Reuters Streetevents, Nov. 11, 2014, at 9 (emphasis added).

161. The following day, November 12, 2014, Davis and Power presented at the Pacific Crest Internet Innovations Conference in New York City (the "Pacific Crest Conference"). The Pacific Crest Conference, which was hosted by Pacific Crest analyst Josh Beck, was attended by financial analysts, investors, and members of the industry, among others. Davis and Power's presentations were streamed live and hosted on the Investor Relations page of LifeLock's website. Replays of the presentation were also made available on the Investor Relations page. During the presentation, Davis represented that LifeLock was at all times in compliance with the FTC Order, described

the process with the FTC as a mere "dialogue" in which the Company was acting "proactively," and dismissively referred to the Burke and Peters lawsuits as "nuisance" proceedings, stating:

> ***Well, certainly, we have operated under an FTC consent decree since 2010. So when we had a couple of whistleblower claims that came up early last year, end of the year before, early last year, or earlier this year, we actually proactively reached out to the FTC to say, we would like to call a meeting. We want to go address this, try to get ahead of it some. We knew there would be a dialogue. That has gone on over the course of this year. We have at least, up to this moment, completed answering all their requests, clarifications, further data. So we have done what is called certify our responses.***
>
> Now, that doesn't mean that they couldn't come back and ask, we want some more data or we want more clarification. But at least at this point, we are at where we have provided the information. We have certified those responses. ***It is basically in their court now. I can't predict what that outcome would look like or when they will decide to give us the feedback or have any discussions with us.***
>
> ***And I will say, we will continue to pursue and defend from this whistleblower claim. One of them was resolved fairly quickly. They were tracked at more of a nuisance kind of claim. But the second one, we will continue to vigorously defend that position. That one will run its course.***

*LOCK – LifeLock Inc at Pacific Crest Internet Innovations Conference*, Thomson Reuters Streetevents, Nov. 12, 2014, at 7 (emphasis added).

162. The statements in paragraphs 153 through 161 were knowingly, or with deliberate recklessness, false and misleading because Defendants knew that the FTC was not merely engaged in an innocent "dialogue" or non-threatening "inquiry," or looking at LifeLock as part of an industry-wide, run-of-the-mill regulatory surveillance program. Rather, Defendants knew that the FTC was formally investigating the Company in connection with the contemplated filing of a motion to hold LifeLock in contempt for violating the FTC Order.

163. According to Winston, LifeLock's communications with the FTC in January 2014 were not a merely proactive attempt by the Company to "discuss" the allegations in the whistleblower complaints, given that Lifelock: (1) was subject to the injunctive terms and conditions of the FTC Order; (2) was aware that the FTC considered

alerts to be an area of interest and would be asking for information and documents; and (3) was urged to enter a litigation hold on "any documents relevant to Lifelock Alerts." In accordance with standard FTC enforcement procedures, Defendants knew or with deliberate recklessness disregarded that LifeLock already had become the subject of a formal FTC investigation, the end result of which was likely to be significant penalties and/or changes in operating procedure.

164. Defendants also knew that the Burke and Peters actions were neither nuisance proceedings nor their allegations tainted by their employment terminations. As discussed above in paragraphs 17 and 66 through 67, Defendants knew that the FTC was using the two complaints as the basis for their investigation, or contemplated investigation, of the Company, and that as a result, the FTC considered the allegations to be sufficiently detailed and credible to warrant an investigation. In fact, LifeLock and the FTC each used the Burke and Peters Compls. as the bases for discussion during the January 17th meeting: the former requested use of the Burke complaint and the latter used the Peters Compl. as an additional predicate for discussion.

### D. The Truth About LifeLock's Failure to Provide Adequate Identity Protection Services and the Severity of the FTC Investigation Begins to Emerge

165. The market began to learn of Defendants' fraud in February 2015, when LifeLock announced that it had accrued a $20 million legal reserve for a possible settlement with the FTC regarding LifeLock's compliance with the FTC Order – which was a decree ordering LifeLock from engaging in certain conduct, including conduct relating to the effectiveness of LifeLock's customer alerts and the effectiveness of its security system.

166. On February 10, 2015, LifeLock made a partial corrective disclosure in a Form 8-K filed with the SEC and in a press release later that day. In the press release, LifeLock represented to the market that it had accrued an additional $20 million in legal reserves "***for a possible settlement with the Federal Trade Commission of their inquiry into our compliance with our 2010 FTC Consent Decree.***"

167. That same day on an earnings call with analysts after the market closed, Defendants continued to downplay the nature and severity of the FTC's investigations into what LifeLock knew were problems with alerts and security (based on its email exchange with the FTC and its own knowledge of its internal systems), and also downplayed the pending enforcement action. During the call Davis reiterated that Lifelock had "***made a settlement offer of $20 million and as a result, have set up a legal reserve that you can see reflected in our financial statements.***" *LOCK – Q4 2014 LifeLock Inc. Earnings Call*, Thomson Reuters Streetevents, Feb. 10, 2015, at 3 (emphasis supplied).

168. Power went on to state:

> ***As Todd mentioned through these discussions we made a settlement offer to the FTC staff in the order of $20 million. While we have not come to terms with the FTC as of yet, and our dialog continues, we have reached the point, based on our preliminary discussions with the FTC staff, that we can make a reasonable assessment of the potential impact. At this point, we estimate the potential range of outcomes to be between $20 million and $100 million.***

*Id*. at 6 (emphasis added).

169. Following these statements, LifeLock's stock price fell from $15.33 share at the close on February 10, 2015, to $14.34 per share at the close on February 11, 2015, a drop of 6.46% on heavy volume.

170. The scope and severity of the conduct related to the FTC investigation and the possible settlement as a result of that conduct were of particular importance to investors. One analyst participating on the February 10, 2015 earnings call, Scott Zeller of Needham & Company asked:

> Could we go back to the provision for legal? If you could comment just from a high level, I think a number of investors are probably wondering what the scope of this would include. So maybe Todd or Chris, if you could just help us from a high level understanding what this might cover out of what is out there, legally, right now that needs to be dealt with?

*Id*. at 12.

171. According to Winston, settlement discussions do not occur between the FTC staff and targets of investigations unless and until the FTC staff has decided that an enforcement proceeding is warranted on the grounds that the FTC has "reason to believe" that a violation has occurred, a standard that is taken very seriously at the FTC and requires a significant level of proof, especially where the FTC staff is seeking to initiate a contempt proceeding. Indeed, according to Winston, under the standard FTC staff settlement procedure, the FTC staff makes the first offer: once it believes that an enforcement proceeding is appropriate because a violation is likely to have occurred, the FTC staff arrives at a settlement figure that then must be approved by the Director of the FTC Bureau of Consumer Protection and that is then presented to the company, along with a draft complaint and consent decree. In over 35 years of experience dealing with hundreds of the same type of settlement negotiations, Winston could not recall one occurrence where the company made the initial settlement offer. Even if LifeLock rather than the FTC made the initial settlement offer, Defendants would not have offered to pay tens of millions of dollars to the FTC, unless they knew an enforcement proceeding was imminent.

172. The partial disclosures contained in paragraphs 166 through 168 were nevertheless false and misleading in that Defendants failed to disclose the scope of wrongdoing that the FTC was investigating. Defendants knew, or with deliberate recklessness failed to know, that the conduct being investigated by the FTC involved the Company's ecosystem – providing near real-time alerts – and protecting members' sensitive data. As such, Defendants knew that a motion to hold the Company in contempt would (and did) have a materially adverse impact on LifeLock's core business, *i.e.*, detecting and preventing identity theft and identity fraud before it happens.

**E. The End of the Class Period**

173. On July 21, 2015, the FTC issued a press release entitled, "FTC Takes Action Against LifeLock for Alleged Violations of 2010 Order." Therein, the FTC, in

relevant part, announced to the public – including the securities markets – that it had determined through its investigation that there was reason to believe that (a) LifeLock did ***not*** consistently provide "real-time" alerts as represented, and (b) LifeLock was ***not*** in compliance with the FTC Order (emphasis added):

> The Federal Trade Commission today asserted that LifeLock violated a 2010 settlement with the agency and 35 state attorneys general by continuing to make deceptive claims about its identity theft protection services, and by failing to take steps required to protect its users' data.
>
> In documents filed with the U.S. District Court for the District of Arizona, the FTC charged that LifeLock failed to live up to its obligations under the 2010 settlement, and asked the court to impose an order requiring LifeLock to provide full redress to all consumers affected by the company's order violations.
>
> "It is essential that companies live up to their obligations under orders obtained by the FTC," said Jessica Rich, Director of the FTC's Bureau of Consumer Protection. "If a company ***continues*** with practices that violate orders and harm consumers, we will act."
>
> The 2010 settlement stemmed from previous FTC allegations that LifeLock used false claims to promote its identity theft protection services. The settlement barred the company and its principals from making any further deceptive claims; required LifeLock to take more stringent measures to safeguard the personal information it collects from customers; and required LifeLock to pay $12 million for consumer refunds.
>
> The FTC charged today that in spite of these promises, from ***at least*** October 2012 through March 2014, LifeLock violated the 2010 Order by: 1) failing to establish and maintain a comprehensive information security program to protect its users' sensitive personal data, including credit card, social security, and bank account numbers; *2)* ***falsely advertising that it protected consumers' sensitive data with the same high-level safeguards as financial institutions;*** and 3) failing to meet the 2010 order's recordkeeping requirements.
>
> ***The FTC also asserts that from at least January 2012 through December 2014, LifeLock falsely claimed it protected consumers' identity 24/7/365 by providing alerts "as soon as" it received any indication there was a problem.***
>
> Details of the FTC's action against the company were filed under seal. The court will determine which portions of the case will be unsealed.
>
> The Commission vote to file the application for a show cause order was 4-1, with Commissioner Maureen K. Ohlhausen voting no.

174. On this news, shares of LifeLock declined $7.91 per share, nearly 50%, after mid-day trading halts, to close on July 21, 2015, at $8.15 per share, on unusually heavy volume.

**F. Post-Class Period Events**

175. At the RBC Capital Markets TMT Investor Conference on November 10, 2015, Davis – after repeating the claim that LifeLock sends customers instantaneous alerts of potentially fraudulent transactions "while you're standing in the store," *LOCK – LifeLock Inc. at RBC Capital Markets TMT Investor Conference*, Thomson Reuters Streetevents, Nov. 10, 2015, at 2 – announced a "preliminary agreement with the staff that we'll go to the commission of the FTC." *Id.* at 3. Davis acknowledged that "we know that we had some impact from" the commencement of the FTC contempt proceeding. *Id.*

176. On October 28, 2015, along with its third quarter results, the Company announced that it reached tentative agreements to settle lawsuits with the FTC and consumers who sued the Company for a combined $116 million. As a result of this announcement, LifeLock's stock price increased from $9.69 per share at the close on October 28, 2015, to $13.94 per share at the close on October 29, 2015, an increase of 43.86% on heavy volume.

177. In an SEC Form 8-K filed on November 25, 2015, LifeLock announced that its Chief Legal Strategist, Clarissa Cerda, was leaving the Company.

178. Then, in an SEC Form 8-K filed on January 20, 2016, LifeLock announced that Defendant Davis was resigning from the position of Chief Executive Officer of the Company and as Chairman of the Company's Board of Directors effective March 1, 2016.

179. In the same 8-K, LifeLock announced that Defendant Schneider was appointed to the position of Chief Executive Officer and President of the Company,

effective March 1, 2016. Defendant Schneider was also appointed as a member of the Board of Directors.

180. Finally, in an SEC Form 8-K filed on March 7, 2016, LifeLock announced that Defendant Power was stepping down from his position of Chief Financial Officer and would be employed by the Company in a non-executive employee advisory role until December 31, 2016.

## CLASS ACTION ALLEGATIONS

181. Lead Plaintiffs bring this action on their own behalf and as a class action pursuant to Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure on behalf of the Class (*i.e.*, all persons and entities who purchased shares of LifeLock's publicly traded common stock and/or call options, and/or sold LifeLock's publicly traded put options, and were damaged thereby), during the Class Period (*i.e.*, from July 30, 2014 through July 21, 2015, inclusive). Excluded from the Class are the Excluded Parties (*i.e.*, Defendants; members of the immediate families of the Individual Defendants; LifeLock's subsidiaries and affiliates, including LifeLock's employee retirement and benefit plan(s); any person who is or was an officer or director of LifeLock or any of LifeLock's subsidiaries or affiliates during the Class Period; any entity in which any Defendant has a controlling interest; and the legal representatives, heirs, successors and assigns of any such excluded person or entity).

182. The members of the Class are so numerous that joinder of all members is impracticable. During the Class Period, LifeLock had between 92 million to 95 million shares of common stock outstanding and actively trading on the NYSE with the ticker symbol "LOCK." While the exact number of Class members is unknown to Lead Plaintiffs at this time and can only be ascertained through appropriate discovery, Lead Plaintiffs believe that the proposed Class numbers in the thousands and is geographically widely dispersed. Record owners and other members of the Class may be identified from records maintained by LifeLock or its transfer agent and may be notified of the pendency

of this action by mail, using a form of notice similar to that customarily used in securities class actions.

183. Lead Plaintiffs' claims are typical of the claims of the members of the Class. All members of the Class were similarly affected by Defendants' allegedly wrongful conduct in violation of the Exchange Act as complained of herein.

184. Lead Plaintiffs will fairly and adequately protect the interests of the members of the Class. Lead Plaintiffs have retained counsel competent and experienced in class and securities litigation.

185. Common questions of law and fact exist as to all members of the Class, and predominate over any questions solely affecting individual members of the Class. The questions of law and fact common to the Class include:

(a) whether the federal securities laws were violated by Defendants' acts and omissions as alleged herein;

(b) whether the statements made to the investing public during the Class Period contained material misrepresentations or omitted to state material information;

(c) whether and to what extent the market price of LifeLock's common stock and call options were artificially inflated, and the market price of LifeLock's put options artificially deflated, during the Class Period because of the material misstatements alleged herein;

(d) whether Defendants acted with the requisite level of scienter;

(e) whether the Individual Defendants were controlling persons of LifeLock;

(f) whether reliance may be presumed pursuant to the fraud-on-the-market doctrine; and

(g) whether the members of the Class have sustained damages as a result of the conduct complained of herein and, if so, the proper measure of damages.

186. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy because, among other things, joinder of all members of the Class is impracticable. Furthermore, because the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigations make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in the management of this action as a class action.

**LOSS CAUSATION**

187. During the Class Period, as detailed herein, Defendants engaged in a scheme to deceive the market and a course of conduct that artificially inflated the price of LifeLock securities and operated as a fraud or deceit on Class Period purchasers of LifeLock securities by failing to disclose and misrepresenting the adverse facts detailed herein. As Defendants' prior misrepresentations and fraudulent conduct were disclosed and became apparent to the market, the price of LifeLock common stock and call options declined significantly, and the price of put options rose significantly, as the prior artificial inflation was removed from the Company's stock price.

188. As a result of their purchases of LifeLock securities during the Class Period, Lead Plaintiffs and the other Class members suffered economic loss, *i.e.*, damages, under the federal securities laws. Defendants' false and misleading statements had the intended effect and caused LifeLock securities to trade at artificially inflated levels throughout the Class Period, with LifeLock's common stock reaching as high as $19.15 per share on December 31, 2014.

189. By making the false and misleading statements to investors detailed herein, Defendants presented a false and misleading picture of LifeLock's business and operations. As the truth about the Company was revealed to the market and/or as the risks misrepresented and concealed by Defendants materialized, the price of LifeLock securities fell significantly. These declines removed the inflation from the price of

LifeLock securities, causing real economic loss to investors who had purchased LifeLock securities during the Class Period.

190. The decline in the price of LifeLock securities after the corrective disclosures came to light were a direct result of the nature and extent of Defendants' fraudulent misrepresentations and omissions being revealed to investors and the market. The timing and magnitude of the price declines in LifeLock securities negate any inference that the loss suffered by Lead Plaintiffs and the other Class members was caused by changed market conditions, macroeconomic or industry factors, or Company-specific facts unrelated to Defendants' fraudulent conduct.

191. During the Class Period, the price of LifeLock stock declined as the true state of LifeLock's business and operations were revealed to the investing public.

192. The economic loss, *i.e.*, damages, suffered by Lead Plaintiffs and the other Class members, was a direct result of Defendants' fraudulent scheme to artificially inflate the price of LifeLock securities and the subsequent significant decline in the value of LifeLock securities when Defendants' prior misrepresentations and other fraudulent conduct were revealed.

## SCIENTER ALLEGATIONS

193. As alleged herein, Defendants acted with scienter in that Defendants knew that the public documents and statements issued or disseminated in the name of the Company were materially false and/or misleading; knew that such statements or documents would be issued or disseminated to the investing public; and knowingly and substantially participated or acquiesced in the issuance or dissemination of such statements or documents as primary violations of the federal securities laws. The Individual Defendants, by virtue of their receipt of information reflecting the true facts regarding LifeLock, their control over, and/or receipt and/or modification of LifeLock's allegedly materially misleading misstatements and/or their associations with the

Company, which made them privy to confidential proprietary information concerning LifeLock, participated in the fraudulent scheme alleged herein.

194. These misrepresentations concern LifeLock's core operations. Provision of alerts to consumer customers, and other matters at issue in the FTC's investigation, were at the very heart of LifeLock's business – *i.e.*, the LifeLock ecosystem. Senior management – including Davis, Power and Schneider – knew the details of, and were intimately involved in, LifeLock's core operations.

195. During the Class Period, identity theft and fraud detection and protection were LifeLock's "core business." Indeed, it was the primary service LifeLock offered. Defendants' constant emphasis on instantaneous alerts that enable consumers to intervene in fraudulent transactions before they are completed shows that this service was a cornerstone of LifeLock's business. Similarly, the other matters covered by the FTC Order, including security protection of personal customer data, were other aspects of the primary service LifeLock provided.

196. As such, LifeLock's senior personnel knew the details concerning LifeLock's customer alerts and customer data security protection. LifeLock was not a large operation, and Defendants Davis, Power and Schneider, LifeLock's CEO, CFO and President, had "hands-on" involvement in day-to-day operations. Moreover, according to CW 5 Defendant Schneider took over the member services side of the business after Defendant Davis had taken a step back to focus on the Company's marketing efforts.

197. According to CW 2, Power led "Operations Review Meetings," held approximately monthly, for all LifeLock's departments (including Information Technology, Marketing, the Call Center, Finance, and all the other departments at LifeLock). CW 2 stated that, at these meetings, systems issues such as data security protection, and problems with the Customer Service Department (such as those that led LifeLock to engage in "throttling"), were discussed. Moreover, CW 2 stated that these

meetings were attended by all LifeLock department directors, and sometimes by Davis and Schneider.

198. Defendants' scienter is further established by factual allegations set forth above. The allegations set forth in paragraphs 119 through 130 establish that LifeLock's senior management (including Hilary Schneider) were apprised of problems with "stale" alerts and that LifeLock purposely elected to throttle customer alerts. CW 5 created reports that detailed statistics related to the staleness of alerts and these reports were sent to Defendant Schneider on a monthly basis and were also sent to the Company's senior management. Moreover, CW 5 confirmed that Defendant Schneider acknowledged the Company's system stability and stale alerts issue in May 2015 at a luncheon meeting both CW 5 and Defendant Schneider attended. As the provision of alerts to customers was LifeLock's core business, LifeLock's senior management – including the Individual Defendants – knew of and were involved in the making of the decision to suppress and delay customer alerts, contrary to Defendants' constant representations that LifeLock provided "proactive" "near real-time" alerts. LifeLock's senior management – including the Individual Defendants – knew, or with deliberate recklessness disregarded, that LifeLock failed to send out near real-time alerts to customers.

199. The allegations set forth in Paragraphs 134 through 150 establish that LifeLock's senior management knew of, or with deliberate recklessness disregarded, the serious deficiencies in LifeLock's data security protection of private customer information. Among other things alleged in those Paragraphs, senior management asserted to employees that the Company would not spend the $100 million necessary to bring it into data security compliance; the Company's President told an employee that the Company had other priorities than to remedy its data security problems; and the Company's Director of Internal Audits instructed an employee not to communicate any facts concerning LifeLock's data security problems to auditors. As the protection of the private information of customers was a core business of LifeLock, its senior management

(including the Individual Defendants) knew of, or with deliberate recklessness disregarded, the Company's data security problems.

200. The allegations of Paragraphs 71 through 72, 162 through 164 and 171 through 172 establish, on the basis of facts pled and information supplied by Lead Plaintiffs' Consultant, that Defendants knew, or with deliberate recklessness disregarded, that prior to and throughout the Class Period, LifeLock was the subject of a formal FTC investigation, the end result of which was likely to be significant penalties and/or changes in operating procedure; and that the discussion of settlement meant that an enforcement proceeding, the end result of which was likely to be significant penalties and/or changes in operating procedure, was imminent.

**APPLICABILITY OF PRESUMPTION OF RELIANCE (FRAUD-ON-THE-MARKET DOCTRINE)**

201. The market for LifeLock's securities was open, well-developed and efficient at all relevant times. As a result of the materially false and/or misleading statements and/or failures to disclose, LifeLock's securities traded at artificially inflated prices during the Class Period. On December 31, 2014, the Company's stock traded at a Class Period high of $19.15 per share. Plaintiffs and other members of the Class purchased or otherwise acquired the Company's securities relying upon the integrity of the market price of LifeLock's securities and market information relating to LifeLock, and have been damaged thereby.

202. During the Class Period, the artificial inflation of LifeLock's securities was caused by the material misrepresentations and/or omissions particularized in this Complaint causing the damages sustained by Plaintiffs and other members of the Class. As described herein, during the Class Period, Defendants made or caused to be made a series of materially false and/or misleading statements about LifeLock's business and operations. These material misstatements and/or omissions created an unrealistically positive assessment of LifeLock and its business and operations, thus causing the price of the Company's securities to be artificially inflated at all relevant times, and when

disclosed, negatively affected the value of the Company securities. Defendants' materially false and/or misleading statements during the Class Period resulted in Plaintiffs and other members of the Class purchasing the Company's securities at such artificially inflated prices, and each of them has been damaged as a result.

203. At all relevant times, the market for LifeLock's securities was an efficient market for the following reasons, among others:

(a) LifeLock's stock met the requirements for listing, and was listed and actively traded on the NYSE, a highly efficient and automated market;

(b) as a regulated issuer, LifeLock filed periodic public reports with the SEC and/or the NYSE;

(c) LifeLock regularly communicated with public investors via established market communication mechanisms, including through regular dissemination of press releases on the national circuits of major newswire services and through other wide-ranging public disclosures, such as communications with the financial press and other similar reporting services; and/or

(d) LifeLock was followed by securities analysts employed by brokerage firms who wrote reports about the Company, and these reports were distributed to the sales force and certain customers of their respective brokerage firms. Each of these reports was publicly available and entered the public marketplace.

204. As a result of the foregoing, the market for LifeLock's securities promptly digested current information regarding LifeLock from all publicly available sources and reflected such information in LifeLock's stock price. Under these circumstances, all purchasers of LifeLock's securities during the Class Period suffered similar injury through their purchase of LifeLock's securities at artificially inflated prices and a presumption of reliance applies.

**NO SAFE HARBOR**

205. The statutory safe harbor provided for forward-looking statements under certain circumstances does not apply to any of the allegedly false statements pleaded in this Complaint. The statements alleged to be false and misleading herein all relate to then-existing facts and conditions. In addition, to the extent certain of the statements alleged to be false may be characterized as forward looking, they were not identified as "forward-looking statements" when made and there were no meaningful cautionary statements identifying important factors that could cause actual results to differ materially from those in the purportedly forward-looking statements. In the alternative, to the extent that the statutory safe harbor is determined to apply to any forward-looking statements pleaded herein, Defendants are liable for those false forward-looking statements because at the time each of those forward-looking statements was made, the speaker had actual knowledge that the forward-looking statement was materially false or misleading, and/or the forward-looking statement was authorized or approved by an executive officer of LifeLock who knew that the statement was false when made.

**COUNT I**

**Violation of § 10(b) of the Exchange Act and Rule 10b-5 Promulgated Thereunder Against All Defendants**

206. Lead Plaintiffs repeat and reallege each and every allegation set forth above as if fully set forth herein.

207. This Count is asserted pursuant to Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder by the SEC against all Defendants.

208. As alleged herein, throughout the Class Period, Defendants, individually and in concert, directly and indirectly, by the use of the means or instrumentalities of interstate commerce, the mails and/or the facilities of national securities exchanges, made untrue statements of material fact and/or omitted to state material facts necessary to make their statements not misleading and carried out a plan, scheme and course of conduct, in violation of Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder.

Defendants intended to and did, as alleged herein, (i) deceive the investing public, including Lead Plaintiffs and members of the Class; (ii) artificially inflate and maintain the prices of LifeLock common stock; and (iii) cause Lead Plaintiffs and members of the Class to purchase LifeLock common stock at artificially inflated prices.

209. The Individual Defendants were individually and collectively responsible for making the false and misleading statements and omissions alleged herein and having engaged in a plan, scheme and course of conduct designed to deceive Lead Plaintiffs and members of the Class, by virtue of having made public statements and prepared, approved, signed and/or disseminated documents that contained untrue statements of material fact and/or omitted facts necessary to make the statements therein not misleading.

210. As set forth above, Defendants made their false and misleading statements and omissions and engaged in the fraudulent activity described herein knowingly and intentionally, or in such a deliberately reckless manner as to constitute willful deceit and fraud upon Lead Plaintiffs and the other members of the Class who purchased LifeLock securities during the Class Period.

211. In ignorance of the false and misleading nature of Defendants' statements and omissions, and relying directly or indirectly on those statements or upon the integrity of the market price for LifeLock securities Lead Plaintiffs and other members of the Class purchased LifeLock securities at artificially inflated prices during the Class Period. But for the fraud, Lead Plaintiffs and members of the Class would not have purchased LifeLock securities at such artificially inflated prices. As set forth herein, when the true facts were subsequently disclosed, the price of LifeLock securities declined precipitously and Lead Plaintiffs and members of the Class were harmed and damaged as a direct and proximate result of their purchases of LifeLock securities at artificially inflated prices and the subsequent decline in the price of that security when the truth was disclosed.

212. By virtue of the foregoing, Defendants are liable to Lead Plaintiffs and members of the Class for violations of Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder.

**COUNT II**

**Violation of § 20(a) of the Exchange Act Against the Individual Defendants**

213. Lead Plaintiffs repeat and reallege each of the allegations set forth above as if fully set forth herein.

214. This Count is asserted pursuant to Section 20(a) of the Exchange Act against each of the Individual Defendants.

215. As alleged above, LifeLock violated Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder by making materially false and misleading statements in connection with the purchase and sale of LifeLock's securities and by participating in a fraudulent scheme and course of business or conduct throughout the Class Period. This fraudulent conduct was undertaken with scienter and the Company is charged with the knowledge and scienter of each of the Individual Defendants who knew of or acted with deliberate reckless disregard of the falsity of the Company's statements and the fraudulent nature of its scheme during the Class Period.

216. As set forth above, the Individual Defendants were controlling persons of LifeLock during the Class Period, due to their senior executive positions with the Company and their direct involvement in the Company's day-to-day operations, including its business practices and compliance with the FTC Order.

217. By virtue of the foregoing, the Individual Defendants each had the power to influence and control, and did influence and control, directly or indirectly, the decision-making of LifeLock, including the content of its public statements with respect to its business practices and compliance with the FTC Order, especially as related to the practice of throttling, LifeLock's adherence to the highest level, Level 1, of the Payment Card Industry Data Security Standard and the Company's failure to establish and

maintain a comprehensive information security program to protect its users' sensitive personal data.

218. These Individual Defendants acted knowingly and intentionally, or in such a deliberately reckless manner as to constitute willful fraud and deceit upon Lead Plaintiffs and the other members of the Class who purchased LifeLock securities during the Class Period.

219. In ignorance of the false and misleading nature of the Company's statements and omissions, and relying directly or indirectly on those statements or upon the integrity of the market prices for LifeLock securities, Lead Plaintiffs and other members of the Class purchased LifeLock securities at an artificially inflated price during the Class Period. But for the fraud, Lead Plaintiffs and members of the Class would not have purchased LifeLock securities at artificially inflated prices. As set forth herein, when the true facts were subsequently disclosed, the price of LifeLock common stock declined precipitously and Lead Plaintiffs and members of the Class were harmed and damaged as a direct and proximate result of their purchases of LifeLock securities stock at artificially inflated prices and the subsequent decline in the price of those securities when the truth began to be disclosed.

220. By reason of the foregoing, the Individual Defendants are liable to Lead Plaintiffs and the members of the Class as controlling persons of LifeLock in violation of Section 20(a) of the Exchange Act.

## PRAYER FOR RELIEF

**WHEREFORE,** Lead Plaintiffs respectfully pray for judgment as follows:

A. Determining that this action is a proper class action maintained under Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure, certifying Lead Plaintiffs as class representatives, and appointing Labaton Sucharow LLP and Bernstein Liebhard LLP as class counsel pursuant to Rule 23(g);

B. Declaring and determining that Defendants violated the Exchange Act by reason of the acts and omissions alleged herein;

C. Awarding Lead Plaintiffs and the Class compensatory damages against all Defendants, jointly and severally, in an amount to be proven at trial together with prejudgment interest thereon;

D. Awarding Lead Plaintiffs and the Class their reasonable costs and expenses incurred in this action, including but not limited to attorney's fees and costs incurred by consulting and testifying expert witnesses; and

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

## JURY DEMAND

Lead Plaintiffs demand a trial by jury of all issues so triable.

Dated: October 14, 2016

**LABATON SUCHAROW LLP**

By: /s/ James W. Johnson
JAMES W. JOHNSON
CAROL C. VILLEGAS
BARRY MICHAEL OKUN
MARISA N. DEMATO *(pro hac vice forthcoming)*
JAMES T. CHRISTIE
140 Broadway
New York, NY 10005
Telephone: (212) 907-0700
Facsimile: (212) 818-0477
Email: jjohnson@labaton.com
cvillegas@labaton.com
bokun@labaton.com
mdemato@labaton.com
jchristie@labaton.com

**BERNSTEIN LIEBHARD LLP**
STANLEY D. BERNSTEIN
MICHAEL S. BIGIN
JOSEPH R. SEIDMAN, JR.
PETER J. HARRINGTON
10 East 40th Street
New York, NY 10016
Telephone: (212) 779-1414
Facsimile: (212) 779-3218
Email: Bernstein@bernlieb.com
Bigin@bernlieb.com
Seidman@bernlieb.com
Harrington@bernlieb.com

*Counsel for the Oklahoma Police Pension and Retirement System and the Oklahoma Firefighters Pension and Retirement System and Proposed Lead Counsel for the Class*

**BONNETT, FAIRBOURN, FRIEDMAN & BALINT, P.C.**
Kimberly C. Page (AZ # 022631)
2325 E. Camelback Road, #300
Phoenix, AZ 85016
Telephone: (602)-274-1100
Facsimile: (602) 274-1199
Email: kpage@bffb.com

*Liaison Counsel for the Oklahoma Police Pension and Retirement System and the Oklahoma Firefighters Pension and Retirement System and Liaison Counsel for the Class*

**CERTIFICATE OF SERVICE**

I hereby certify that on October 14, 2016, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the e-mail addresses denoted on the Electronic Mail notice list, and I hereby certify that I have mailed the foregoing document or paper via the United States Postal Service to the non-CM/ECF participants indicated on the Manual Notice list.

I certify under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

/s/ James W. Johnson
James W. Johnson