

Gallagher & Kennedy, P.A.
2575 East Camelback Road
Phoenix, Arizona 85016-9225
(602) 530-8000

1 Paul L. Stoller (016773)
paul.stoller@gknet.com
 2 Lincoln Combs (025080)
lincoln.combs@gknet.com
 3 GALLAGHER & KENNEDY, P.A.
 2575 E. Camelback Road
 4 Phoenix, AZ 85016
 Telephone: 602-530-5000
 5 Facsimile: 602-530-8500

6 Randall K. Pulliam
rpulliam@cbplaw.com
 7 E. Lee Lowther III
llother@cbplaw.com
 8 CARNEY BATES & PULLIAM, PLLC
 519 W. 7th St.
 9 Little Rock, AR 72201
 Telephone: (501) 312-8500
 10 Facsimile: (501) 312-8505
 (*pro hac vice* applications to be filed)

11 Irwin B. Levin
ilevin@cohenandmalad.com
 12 Richard E. Shevitz
rshevitz@cohenandmalad.com
 13 Vess A. Miller
vmiller@cohenandmalad.com
 14 Lynn A. Toops
ltoops@cohenandmalad.com
 15 COHEN MALAD, LLP
 One Indiana Square, Suite 1400
 16 Indianapolis, IN 46204
 Telephone: (317) 636-6481
 17 Facsimile: (317) 636-2593
 18 (*pro hac vice* applications to be filed)

19 Counsel for Plaintiffs and
 the Putative Class

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

22 JOE WEINGARTEN and DARRELL
 23 HUNTER, on behalf of themselves and
 all others similarly situated,

24 Plaintiffs,

25 v.

26 LIFELOCK, INC.,

27 Defendant.
 28

Case No. _____

CLASS ACTION COMPLAINT

1. VIOLATIONS OF THE ARIZONA CONSUMER FRAUD ACT (ARIZ. REV. STAT. § 44-1522(A))
2. BREACH OF CONTRACT
3. DECLARATORY JUDGMENT
4. UNJUST ENRICHMENT

1 For their Complaint, Plaintiffs Joe Weingarten and Darrell Hunter, on behalf of
2 themselves and all other persons similarly situated, against Defendant LifeLock, Inc.
3 (“Defendant” or “LifeLock” or the “Company”) allege as follows:

4 **INTRODUCTION**

5 1. LifeLock aggressively markets “identity theft protection” via numerous
6 channels including television, radio, online, and contracted affiliates. However, LifeLock
7 fails to deliver a product that fulfills the numerous promises made in its advertisements.

8 2. On two prior occasions, the Federal Trade Commission (“FTC”) has sued
9 LifeLock related to false representations made in LifeLock advertising. As a result of
10 those FTC suits, LifeLock is enjoined from making misleading statements concerning the
11 nature of its service. Despite the clear prohibition, LifeLock continues to market its
12 product in a manner that misstates the actual services it is able to offer to consumers.

13 3. LifeLock offers three levels of service – Standard, Advantage, and Ultimate
14 Plus. The price ranges from \$9.99 per month for Standard up to \$29.99 per month for
15 Ultimate Plus. All three plans share certain purported benefits, including the “Million
16 Dollar Protection Package” and “LifeLock Identity Alert.” The more expensive plans
17 offer additional purported services such as notifications about “Cash Withdrawals,
18 Transfers and Large Purchases” and “New Bank Account Applications.”

19 4. All three of these plans claim to offer two types of protection from identity
20 theft: (1) protection and notification if a plan member’s personally identifiable
21 information (“PII”) is stolen and/or used to fraudulently obtain credit, and (2)
22 reimbursement and assistance on the back end if indeed a plan member is the victim of
23 identity theft. LifeLock states “Identity theft protection is hard. We make it easy for you.”

24 5. In reality, LifeLock does not deliver on these advertising promises. As a
25 result, Plaintiffs paid hundreds of dollars for a product that not only provided them no
26 meaningful protection from identity theft, but actually created a false sense of security that
27 their interests were being monitored. Further, after Plaintiff Weingarten personally
28 uncovered that his social security number and personal credit was fraudulently used to

1 open credit accounts on multiple occasions, LifeLock refused to offer assistance in fixing
2 the problem.

3 6. LifeLock did not notify Plaintiff Weingarten that a false change of address
4 had been filed under his name with the United States Postal Service (“USPS”). In the
5 listed benefits of each of the three plans, LifeLock specifically lists “Address Change
6 Verification” as an area that it monitors, stating “LifeLock lets you know of changes in
7 address requests linked to your identity.” In fact, LifeLock is unable to accurately track
8 this information and, as a result, did not notify Plaintiff Weingarten that credit accounts
9 were opened in his name using this false change of address.

10 7. Once Plaintiff Weingarten uncovered these accounts, he notified LifeLock
11 and requested assistance in repairing his credit. While LifeLock claims “if you become a
12 victim of identity theft, a U.S.-based Identity Restoration Specialist will be dedicated to
13 your case from start to finish,” LifeLock gave Plaintiff Weingarten no assistance in
14 closing these accounts, paying costs associated with them, or otherwise clearing up the
15 damage done to his credit. Likewise, LifeLock failed to provide identity theft victim
16 assistance to Plaintiff Darrell Hunter when he disputed a credit inquiry.

17 8. The fact that LifeLock did not uncover these uses of Plaintiff Weingarten’s
18 address and personal credit to his detriment (either before or after it occurred) is not an
19 anomaly. In fact, it is typical of LifeLock service, as the company monitors only a tiny
20 percentage of all sources of credit applications – i.e., banks, credit cards, retail. As a
21 result, LifeLock has no ability to deliver upon the advertising promises it makes because
22 the vast majority of credit applications (and thus fraudulent account openings) are not
23 monitored by LifeLock.

24 9. In light of LifeLock’s history of making advertising claims it had no ability
25 to honor, the FTC and 35 state Attorneys General sued LifeLock in this district. In order
26 for LifeLock to continue to operate, it agreed to a permanent injunction to modify its
27 advertising language. LifeLock is presently violating that injunction (the “FTC Permanent
28 Injunction”) in multiple ways by misrepresenting the true nature of its product.

1 or “yours”), and describe the terms under which you agree to
2 use the LifeLock identity programs, including any applicable
3 Stolen Identity Insurance (the “Protection Programs”), credit
4 monitoring service (the “Credit Monitoring Service”) and any
5 other service or product which may be made available to you
6 by us for which you have registered or enrolled or have been
7 registered or enrolled by an authorized third party (collectively
8 the “Services” and individually a “Service”).

9 22. In addition, the Service Terms provide as follows:

10 The Service Terms and any Services provided hereunder will
11 be governed by the laws of the State of Arizona, without
12 regard to any laws that would direct the choice of another
13 state’s laws and, where applicable, will be governed by the
14 federal laws of the United States.

15 23. In sum, LifeLock customers are charged and pay between \$10 and \$30
16 dollars a month in Membership Fees for the Company to monitor their identities and to
17 provide identity theft victim assistance, but as discussed, LifeLock falsely and
18 misleadingly advertises and sells its services and does not provide the promised services.

19 **FACTUAL ALLEGATIONS SPECIFIC TO NAMED PLAINTIFFS**

20 A. Plaintiff Joe Weingarten

21 24. After viewing several of LifeLock’s pervasive television and online
22 advertisements, Plaintiff Joe Weingarten became a member of LifeLock on March 18,
23 2016. Since his enrollment, and based on LifeLock’s representations and promises,
24 Plaintiff Weingarten has paid LifeLock a fee of approximately \$10 per month for
25 LifeLock’s Standard Plan.

26 25. In March or April 2017, an identity thief opened a credit card with Bank of
27 America in Plaintiff Weingarten’s name and tried to open an account with the Navy Credit
28 Union using his identity. The identity thief also successfully submitted a change of
address for Plaintiff Weingarten with the USPS. LifeLock did not alert Plaintiff
Weingarten of any of these three events.

As a result of a notification from Bank of America, Plaintiff Weingarten
was able to stop the Bank of America credit card and inform the USPS of the illegal
change of address.

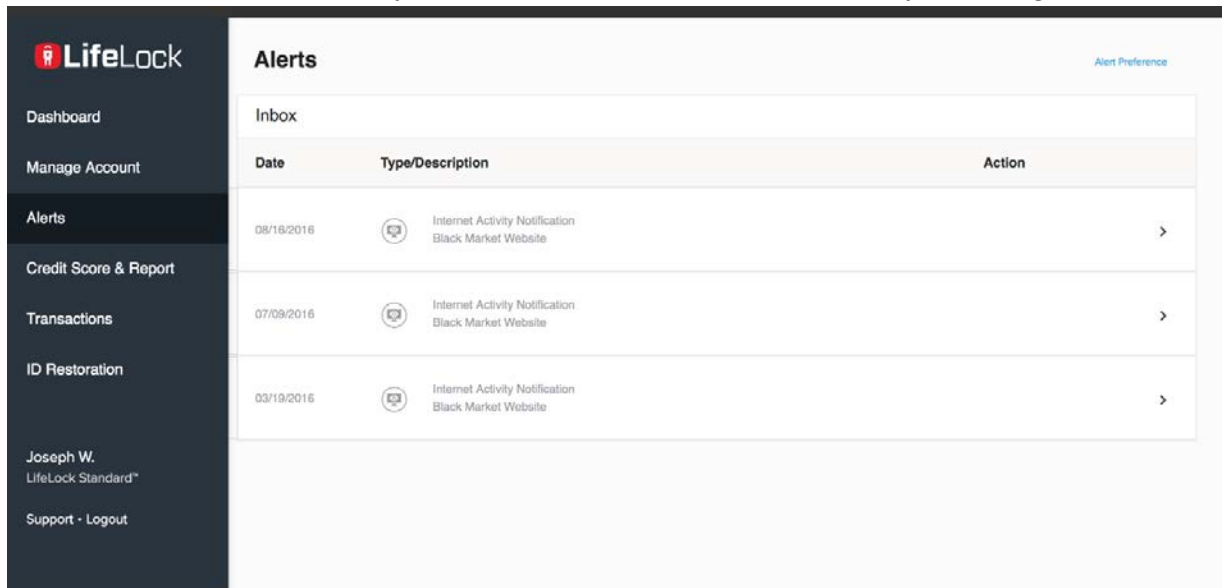
1 27. After receiving the notification from Bank of America, Plaintiff Weingarten
2 obtained a credit report from Experian and discovered that the identity thief had tried to
3 open an account with Navy Federal Credit Union.

4 28. That Experian credit report also revealed that the identity thief tried to
5 change Plaintiff Weingarten's address with Experian. LifeLock did not notify Plaintiff
6 Weingarten of this address change linked to Plaintiff Weingarten's identity.

7 29. When Plaintiff Weingarten notified LifeLock about these multiple events of
8 identity theft, the LifeLock representative tried to sell Plaintiff Weingarten a more
9 expensive LifeLock plan instead of talking to Plaintiff Weingarten about or providing the
10 services outlined on LifeLock's website, such as identity theft restoration and
11 reimbursement for losses.

12 30. Plaintiff Weingarten also had two checks stolen, one of which he stopped
13 with a \$35 fee and another that was used to purchase merchandise through eBay.
14 LifeLock did not notify him of any of these identity theft events.

15 31. On April 11, 2017, Plaintiff Weingarten checked the Alerts section of his
16 LifeLock account and the only alerts on his account were from July and August 2016:

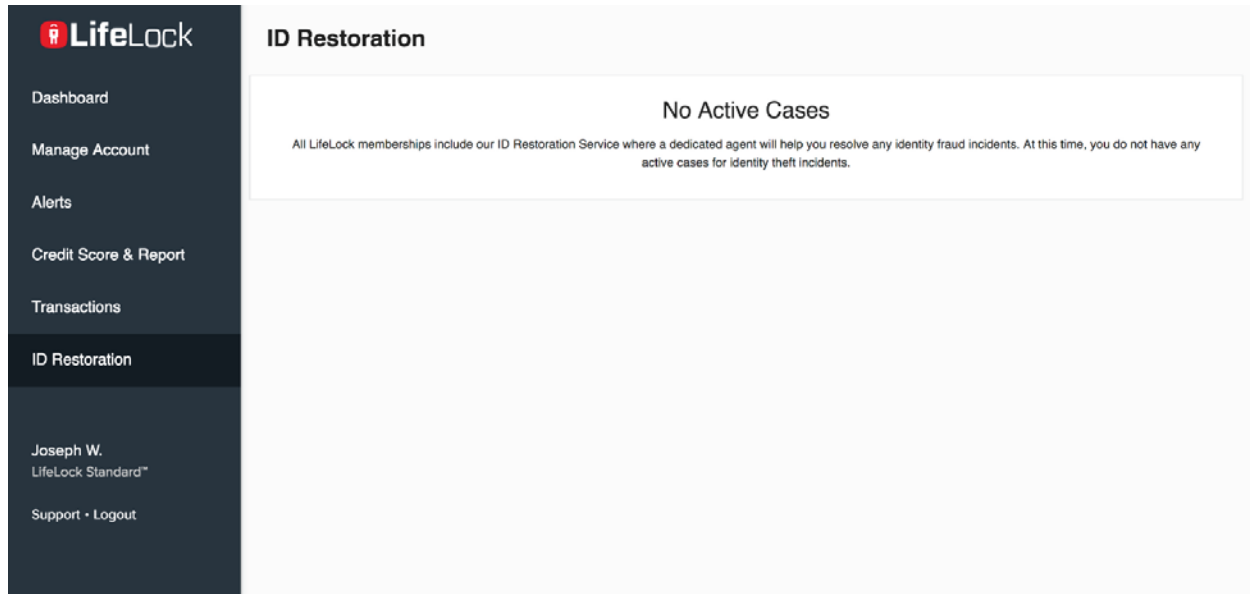


The screenshot shows the LifeLock Alerts section. On the left is a dark sidebar with navigation options: Dashboard, Manage Account, Alerts (highlighted), Credit Score & Report, Transactions, ID Restoration, and user information for Joseph W. LifeLock Standard*. On the right, the Alerts section is titled 'Alerts' and includes an 'Alert Preference' link. Below the title is an 'Inbox' table with three rows of alerts:

Date	Type/Description	Action
08/16/2016	Internet Activity Notification Black Market Website	>
07/09/2016	Internet Activity Notification Black Market Website	>
03/19/2016	Internet Activity Notification Black Market Website	>

17
18
19
20
21
22
23
24
25
26
27 32. On April 11, 2017, Plaintiff Weingarten checked the ID Restoration portion
28 of his LifeLock account and it listed no active cases, although multiple instances of

1 identity theft had taken place over a month before, and Plaintiff Weingarten had
 2 personally reported those instances to LifeLock the previous week:



12

13 33. On April 29, 2017, Plaintiff Weingarten's TDCard credit card was not
 14 accepted at Kroger. Plaintiff Weingarten called TDCard and discovered an identity thief
 15 had entered a change of address on Plaintiff Weingarten's account, the USPS had returned
 16 Plaintiff Weingarten's mailed statement to TDCard, and, as a result, TDCard froze
 17 Plaintiff Weingarten's account. LifeLock did not notify Plaintiff Weingarten of this
 18 change of address on his credit card account or of the freeze placed on Plaintiff
 19 Weingarten's card by the TDCard.

20 34. On May 8, 2017, Plaintiff Weingarten received a Bank of America Health
 21 Savings Account debit card in his name in the mail for which he did not apply. Bank of
 22 America received an application in his name for that card on May 3, 2017. Bank of
 23 America stopped that card based on Plaintiff Weingarten's alert to them. LifeLock did not
 24 notify Plaintiff Weingarten of this identity theft event.

25 B. Plaintiff Darrell Hunter

26 35. After seeing many of LifeLock's television commercials and further
 27 investigating the company's services online, Plaintiff Darrell Hunter became a member of
 28 LifeLock in 2014 or 2015. Since his enrollment, and based on LifeLock's representations

1 and promises, Plaintiff Hunter pays LifeLock a fee of approximately \$22.50 per month for
2 LifeLock's Ultimate Plan. Plaintiff Hunter's wife pays LifeLock a fee of approximately
3 \$25.00 per month for LifeLock's Ultimate Plan.

4 36. On August 8, 2017, Plaintiff Hunter was alerted by LifeLock of an "Address
5 Change Notification USPS – Redirect Mail." The alert listed the USPS as its "Data
6 Source" and placed the alert category as "Public Records – Address Change." The alert
7 listed the "Move Date" as July 1, 2017, or nearly 40 days prior to LifeLock's notice. The
8 LifeLock alert also noted that "[i]f you did not submit this request, contact the post office
9 immediately for resolution."

10 37. On August 14, 2017, and August 22, 2017, Plaintiff Hunter received another
11 alert from LifeLock that was identical to the alert he received on August 8, 2017.

12 38. Plaintiff Hunter also received an alert from LifeLock entitled "Address
13 Change Notification Found on your TransUnion Credit Report." It informed Plaintiff
14 Hunter to "contact TransUnion immediately or file an online dispute."

15 39. Plaintiff Hunter also received an alert of "Credit Inquiry Alert Found On
16 Your Experian Credit Report" from LifeLock that informed Plaintiff Hunter that on
17 January 3, 2017, CBNA made a "Bank – credit card" inquiry on his Experian credit
18 report. Plaintiff Hunter informed LifeLock that he did not apply for a CBNA credit card
19 and clicked "No, this was not me" in his LifeLock online account. However, LifeLock did
20 nothing in response. Indeed, when Plaintiff Hunter applied for a mortgage several months
21 later in Summer 2017, the issue had not been resolved and Plaintiff Hunter's bank
22 mortgage provider required a letter from LifeLock explaining that it had not yet corrected
23 the issue.

24 **II. LifeLock's History of Marketing, Offering, and Selling Its Products to**
25 **Consumers in an Unfair, Misleading, and Deceptive Manner.**

26 A. LifeLock's Claim of Offering "Comprehensive" Services Grossly
27 Misrepresented the Scope and Effectiveness of Its Network

28 40. In 2008, the FTC filed suit against LifeLock alleging that the Company's
services did not prevent identity theft, as represented, and did not provide many of the

1 protections claimed by LifeLock. In resolution of the claims brought by the FTC,
2 LifeLock and the FTC entered into the FTC Permanent Injunction, wherein LifeLock was
3 “permanently restrained and enjoined” from the following:

- 4 A. **in connection with the advertising**, distributing, promoting,
5 offering for sale, or sale of any product, service, or program
6 designed for the purpose of preventing, mitigating, or
7 recovering from any form of identity theft as defined in 18
8 U.S.C. § 1028, **misrepresenting in any manner, expressly or**
9 **by implication:**
- 10 1. that such product, service, or program provides complete
11 protection against all forms of identity theft by making
12 customers’ personal information useless to identity thieves;
 - 13 2. that such product, service, or program prevents unauthorized
14 changes to customers’ address information;
 - 15 3. that such product, service, or program constantly monitors
16 activity on each of its customers’ consumer reports;
 - 17 4. that such product, service, or program ensures that a customer
18 will always receive a phone call from a potential creditor
19 before a new credit account is opened in the customer’s name;
 - 20 5. **the means, methods, procedures, effects, effectiveness,**
21 **coverage, or scope of such product, service, or program;**
 - 22 6. **the risk of identity theft to consumers;**
 - 23 7. **whether a particular consumer has become or is likely to**
24 **become a victim of identity theft; and/or**
 - 25 8. the opinions, beliefs, findings, or experiences of an individual
26 or group of consumers related in any way to any such product,
27 service, or program.

21 Such products, services, or programs include, but are not
22 limited to, the placement of fraud alerts on behalf of
23 consumers, searching the internet for consumers’ personal
24 data, monitoring commercial transactions for consumers’
25 personal data, identity theft protection for minors, and
26 guarantees of any such product, services, or programs.

- 24 B. misrepresenting in any manner, expressly or by implication,
25 the manner or extent to which they maintain and protect the
26 privacy, confidentiality, or security of any personal
27 information collected from or about consumers.

28 (Emphasis Added.)

1 B. LifeLock Settled a Contempt Action with the FTC for Violating the FTC
2 Permanent Injunction.

3 41. In July 2015, the FTC filed a contempt action against LifeLock for violating
4 the FTC Permanent Injunction.

5 42. Specifically, the FTC alleged the violations included, among others, “falsely
6 advertising that it protected consumers’ sensitive data with the same high-level safeguards
7 as financial institutions” and “falsely claiming it protected customers’ identity 24/7/365
8 by providing alerts ‘as soon as’ it received any indication there was a problem.” *See FTC*

9 *v. LifeLock, Inc.*, No. 2:10-cv-530-JTT, ECF No. 67 at 2 (D. Ariz. Jan. 4, 2016).
10 LifeLock “neither admit[ted] nor denie[d]” those allegations, but instead agreed to settle
11 the contempt action by entering into an agreed order modifying the permanent injunction.
12 *Id.*

13 **III. LifeLock Continues to Materially Misrepresent the Scope of its Services.**

14 A. LifeLock Materially Misrepresents the Scope of its Bank and Credit Card
15 Activity Alerts.

16 43. The FTC Permanent Injunction not only forbids LifeLock from making
17 directly false statements about its product, but also prohibits LifeLock from
18 “misrepresenting in any manner, expressly or by implication.”¹ It is axiomatic that for
19 LifeLock to provide a meaningful service to customers related to bank and credit card
20 activity, then LifeLock must monitor or otherwise have access to information from a wide
21 range and large number of banks and credit card issuers. If LifeLock only was able to
22 learn about a new account opening at a limited number of financial institutions, then the
23 level of protection provided to its plan members would be correspondingly small.

24 44. Indeed, upon information and belief, the number of banks and credit card
25 issuers that LifeLock monitors or about which it otherwise learns of new credit
26 applications is exceedingly small. The impact of this tiny network is that plan members do
27 not have the level of protection against identity theft that LifeLock purports to offer. If a

28 ¹ *Federal Trade Commission v. LifeLock, Inc., et al.*, 2:10-cv-530-NVW, ECF No. 9, at 4
(D. Az. Mar. 15, 2010).

1 LifeLock plan member has his or her personal information stolen and used at a bank that
 2 LifeLock does not monitor, i.e., Bank of America or Navy Federal Credit Union, then the
 3 LifeLock coverage provides no protection whatsoever. While LifeLock advertises that its
 4 customers are protected, the scope of the financial institutions it monitors is so small as to
 5 make those representations false and misleading.

6 B. LifeLock Materially Misrepresents the Scope of its Change-of-Address
 7 Monitoring.

8 45. LifeLock recognizes that “[i]dentity thieves try to divert mail to get
 9 important financial information.” ([https://www.LifeLock.com/products/LifeLock-](https://www.LifeLock.com/products/LifeLock-standard/)
 10 [standard/](https://www.LifeLock.com/products/LifeLock-standard/) (last visited Feb. 22, 2018).)

11 46. LifeLock’s website details the risk consumers face when an identity thief
 12 changes their address:

13 Change of address theft is when thieves steal your personal information by
 14 literally changing your address to an address used by them. The end result is
 15 all of your personal identity information is forwarded directly into the hands
 16 of eagerly waiting thieves.

17 **How Does Change of Address Theft Occur?**

18 The U.S. Postal Service processes over 563 million pieces of mail every
 19 day, giving identity thieves plenty of opportunity to capture your
 20 information using your mail. Typically, thieves first start by collecting
 21 addresses, either online, through the phone book, or driving by homes.
 22 Then they simply complete a change of address form, easily available
 23 online or at the local post office, and reroute all of your mail to their hands.

24 **How Effective is Change of Address Theft?**

25 The change of address theft method was the number one way identity
 26 thieves were able to take over existing accounts in 2010.

27 **Information thieves can collect:**

- 28 • Pre-approved card and loan offers
- Social security number
- Telephone numbers
- Email address
- Bank account information
- Employment history and information
- Other personal information

What thieves can do with this information:

- Identity theft
- Employment-related fraud

- Loan fraud/payday loan fraud
- Bank fraud
- Benefits fraud
- Tax fraud
- Other identity fraud

Change of Address Statistics:

- Over 584 million pieces of mail are processed daily by the US Post Office.
- Using change of address forms was the #1 method of account takeover.

(<https://www.LifeLock.com/education/819/> (last visited Feb. 21, 2018) (citing <http://www.usps.com/communications/newsroom/postalfacts.htm>; Javelin Strategy & Research. “2011 Identity Fraud Survey Report,” February 2011; Federal Trade Commission, “Consumer Sentinel Network Data Book For January – December 2011,” February 2012; Javelin Strategy & Research. “2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier.” February 2012).)

47. LifeLock’s website further explains:

There are ways to commit identity theft offline.

With a name and address, a thief can change your address via U.S. Postal Service and redirect mail to their address of choice With access to your financial mail, the thief may intercept bank statements and credit card offers or bills, then order new checks and credit cards.

This is a form of mail theft.

(<https://www.LifeLock.com/education/can-your-identity-be-stolen-with-only-a-name-and-address/> (last visited Feb. 21, 2018).)

48. Because mail theft is a particularly damaging form of identity theft, and therefore protecting against it is crucial to consumers, LifeLock promises to provide “Address Change Verification” for each of its three plans. LifeLock further promises to monitor “change of USPS mailing address requests.”

1 49. For each of its three plans, LifeLock explicitly promises the following with
2 respect to detecting and alerting its Membership Subscribers of address identity theft, as
3 well as other identity-theft related incidents:

- 4 a. “LifeLock lets you know of changes in address requests linked to your
5 identity.”
- 6 b. “Our products help detect identity-related incidents, alert our members to
7 suspicious activity and address identity theft-related issues on behalf of
8 victims.”
- 9 c. “We proactively monitor identity-related events Alerts are sent to our
10 members through our patented LifeLock Identity Alert® system.”
- 11 d. “LifeLock uses proprietary technology that searches for potential threats to
12 your identity. If we see activity using your personal information, we alert
13 you. If it’s not you, we go to work on your behalf.”
- 14 e. “Our proprietary technology scans millions of transactions every second for
15 threats to your identity.”

16 50. LifeLock states that when it discovers a change of address, it will send the
17 customer an email or text-message alert; or for customers who have chosen to receive
18 telephone alerts, LifeLock represents it will call the customer during local business hours.

19 51. The USPS provides access to its change-of-address data via its NCOALink
20 Production, which is “a secure dataset of approximately 160 million permanent change-of-
21 address (COA) records consisting of names and addresses of individuals, families and
22 businesses who have filed a change of address with the Postal Service. The NCOALink
23 data is provided on a regular basis to companies that have been licensed by the Postal
24 Service.” (<https://postalpro.usps.com/mailing-and-shipping-services/NCOALink> (last
25 visited Mar. 7, 2018).)

26 52. The USPS lists its “Full Service Provider Licensees” that receive “48
27 months of change-of-address (COA) data from the USPS® on a weekly basis.”
28

1 (https://postalpro.usps.com/ncoalink/Full_Service_Provider_Licensees (last visited Mar.
2 7, 2018).) LifeLock is not listed as a “Full Service Provider Licensee.”

3 53. The USPS lists its “Limited Service Provider Licensees” that receive “18
4 months of change-of-address (COA) data from the USPS® on a weekly basis.”

5 (https://postalpro.usps.com/ncoalink/Limited_Service_Provider_Licensees (last visited
6 Mar. 7, 2018).) LifeLock is not listed as a “Limited Service Provider Licensees.”

7 54. Therefore, LifeLock does not directly purchase change-of-address data from
8 the USPS.

9 55. The USPS states that commercial customers, like perhaps LifeLock, can
10 purchase change-of-address data from the licensed USPS service providers on a daily,
11 weekly, monthly, quarterly, or annual basis.

12 56. It is not clear from where, or even if, LifeLock purchases USPS change-of-
13 address data, but it is clear that LifeLock does not purchase it from the USPS, but instead
14 (if at all) from a third party; and LifeLock can only obtain that data on a weekly, monthly,
15 quarterly, or annual basis, not contemporaneously or even daily.

16 57. Moreover, on information and belief, LifeLock either simply does not
17 deliver USPS change-of-address alerts to customers who purchased its Standard Plan or
18 does so only sporadically.

19 58. For customers with more expensive plans, LifeLock allows weeks, if not
20 months, to elapse before it delivers the change-of-address alerts, either because it does not
21 even have the information or because it chooses to delay the alerts or does not have the
22 capacity needed to send the alerts out more frequently.

23 59. In either situation, LifeLock delivers nothing approaching the nearly
24 contemporaneous alerts and “protection” it and its affiliates advertise.

25 60. This is likely because nearly 15 percent of Americans move each year. A
26 relocation requires the consumer to change her address with the USPS, the credit bureaus,
27 and for her many accounts (credit cards, banks, loans, etc.). LifeLock boasts that it has 4.4
28 million subscribers, so each year on average, 660,000 LifeLock Subscribers move, which

1 should trigger millions of alerts by LifeLock to its Subscribers if it was fully delivering on
2 its advertised promise.

3 61. Numerous customers, however, have complained online that LifeLock did
4 not notify them of address changes:

5 Find 2 derogatory accounts on my credit reports (that are not mine). Find
6 home addresses that are not mine on my credit reports. Hmmm, you'd think
7 LifeLock would have noted these events and alerted me. Nope, they didn't.

8 You failed to pick notice an address changes in my family - (first step in
9 having someone commit fraud against you) THANKS FOR NOTHING!
Years of charging me and then you were asleep at the wheel!

10 I subscribed to LifeLock last year under the impression that, as advertised,
11 the company would notify me if there was activity using my personal
12 information in order to detect possible identity fraud. Since that time I have
13 moved and changed the address on almost all credit accounts, had credit
14 approved for a lease for a rental, purchased a vehicle, and who knows what
15 else as I went through a divorce. In that entire time I NEVER received a
notice there was activity using my personal information, although that is
exactly what the company had advertised it would do. When I talked to a
company representative, I was told those banks aren't in our network and car
loans aren't always counted...

16 I have been a LifeLock Customer since early 2010. Since then, I have
17 opened four credit cards and Life lock had no idea. No alert, no nothing. I
18 had gotten letters from the local PD of two Sex offenders in the area which
19 LifeLock missed. I moved to another state, new D.L., new car - which I
20 financed. Was I contacted by LifeLock? NOPE.

21 I have been a member (and my family of 5) for over 10 years. I have not
22 received an alert since 2013. Since then I have bought and sold two houses,
23 opened 2 business, lines of credit, credit cards with large limits and I have
24 never received an alert. When I ask LifeLock they give me the same speech
25 - "We don't partner with all institutions." I get free alerts monthly with
26 AAA. I am about ready to cancel.

27 C. LifeLock Misrepresents the Services It Provides Once Identity Theft Occurs

28 62. While LifeLock makes promises about its abilities to prevent identity theft
that it cannot fulfill, LifeLock further fails to honor its obligations (via advertising and the
customer agreement) with respect to helping its customers who have fallen victim to
identity theft by covering their associated out-of-pocket expenses and reimbursing stolen
funds.

1 63. In its plans, LifeLock touts its “Million Dollar Coverage.” This feature
2 purportedly provides coverage for stolen funds and out-of-pocket expenses of up to
3 \$25,000 for Standard Plan Members, \$100,000 for Advantage Members, and \$1,000,000
4 for Ultimate Plus members.

5 64. Specifically, LifeLock represents it will cover its members “for personal
6 expenses incurred as a result of identity theft, up to the limits of your plan.”

7 65. Similarly, LifeLock promises that “[i]f your money is stolen due to ID theft,
8 we will reimburse you up to the amount provided by your plan.”

9 66. LifeLock further promises to its customers that “if you’re ever victimized by
10 identity theft...a member of our U.S.-Based Identity Restoration Team will be dedicated
11 to your case.” (<https://www.lifelock.com/how-it-works/overview/> (last visited Mar. 14,
12 2018.))

13 67. As discussed above, Plaintiff Weingarten incurred out-of-pocket expenses
14 cancelling his stolen checks. Similarly, LifeLock assigned no member of its Restoration
15 Team to investigate and help remediate the multiple instances of identity theft Plaintiff
16 Weingarten reported in 2017.

17 68. Thus, in addition to not providing Plaintiff Weingarten alerts of the many
18 instances in which his identity was stolen, LifeLock made no efforts to investigate those
19 instances or attempt to alleviate their financial toll.

20 D. LifeLock Misrepresents Its Services Using Affiliate and Shadow Websites

21 69. LifeLock was able to perpetuate its maze-like services through use of its
22 “affiliates.” As part of its marketing campaign, LifeLock uses an affiliate program
23 whereby people and/or businesses create websites and blogs that link to LifeLock.com.
24 The affiliates receive a commission on each enrollment generated from their site or
25 review. Thus, LifeLock’s affiliates were incentivized to perpetuate LifeLock’s advertising
26 and marketing scheme and mislead consumers.

27
28

1 70. On information and belief, LifeLock reviews the materials its affiliates
2 intend to post to ensure it conforms with LifeLock’s advertising guidelines and, if
3 satisfied the materials so conform, approves the “neutral” advertisements for display.

4 71. One such affiliate is Identity Theft Labs, a website which claims for itself “a
5 stellar reputation as the leading and most trusted source for professional reviews of
6 the **best identity protection companies.**”

7 ([https://www.identitytheftlabs.com/?gclid=CjwKCAiA8vPUBRAyEiwA8F1oDKqx-](https://www.identitytheftlabs.com/?gclid=CjwKCAiA8vPUBRAyEiwA8F1oDKqx-3j07fDVjvhv3AsiDUrtwVIjfyX2OrGN674A4mr0tQ-1tgre1IhoCjRUQAvD_BwE)
8 [3j07fDVjvhv3AsiDUrtwVIjfyX2OrGN674A4mr0tQ-1tgre1IhoCjRUQAvD_BwE](https://www.identitytheftlabs.com/?gclid=CjwKCAiA8vPUBRAyEiwA8F1oDKqx-3j07fDVjvhv3AsiDUrtwVIjfyX2OrGN674A4mr0tQ-1tgre1IhoCjRUQAvD_BwE) (last
9 visited Mar. 5, 2018) (emphasis in original).)

10 72. According to this “most trusted source,” LifeLock “monitors 1000s of
11 databases and trillions of data points” to provide its customers “**early notification** of
12 potential identity threats.”

13 73. Identity Theft Labs further assures its readers that “LifeLock **alerts you** by
14 text, email and/or phone (Phone alerts made during normal local business hours)
15 **whenever their system detects your personal information being used** to apply for
16 many forms of credit cards, wireless services, retail credit, utilities, check orders/reorders,
17 mortgage loans, auto loans, and non-credit related payday loans.”

18 74. Another “neutral” affiliate that shills for LifeLock is Identity Theft
19 Protection Bureau. This affiliate is particularly pernicious, because ITPB represents its
20 team as true subject-matter experts with “extensive experience in the identity theft
21 industry and [who] are experts in information security.”

22 (<http://www.itpbureau.com/about-us/> (last visited Mar. 5, 2018).)

23 75. In their review of LifeLock, ITPB’s “experts in information security” make
24 many of the extravagant claims that LifeLock has been enjoined from making as
25 misrepresentations.

26 76. For instance, ITPB praises LifeLock’s “ID Network,” which “covers close
27 to 100% of Americans monitoring over a trillion data points and spanning all industries
28

1 from cell phone applications to ecommerce transactions to **change of address.**"

2 (Emphasis added.)

3 77. This "Real Time Data," ITPB continues, gives LifeLock "an up-to-the-
4 minute view of event, consumer, and identity risk."

5 78. LifeLock's up-to-the-minute data, in turn, fuels its "best in class alerts,"
6 through which LifeLock "notifies customers of identity misuse."

7 79. Further stoking customers' expectations that these alerts occur in real time
8 and might actually prevent identity theft—instead of providing a mere after-the-fact
9 announcement—IPTB misinforms customers that an alert is "not just an alert as these
10 notifications are interactive and require the customer (you) to verify the transaction." Put
11 another way, ITPB represents that a customer could choose not to verify the transaction
12 and thwart the would-be identity thief.

13 80. Worse still, LifeLock maintains, either itself or through affiliates, a series of
14 shadow websites that use LifeLock's insignia and appear as though they are maintained
15 by LifeLock.

16 81. LifeLock.**org**—as opposed to the official website LifeLock.**com**—is a prime
17 example of this practice. On that website, LifeLock represents without compunction that
18 its "theft protection services help prevent all forms of identity theft." Moreover, this
19 website states LifeLock's "[t]echnology monitors and alerts members to threats to their
20 personal information to help stop identity theft before it happens."

21 82. Another shadow website through which LifeLock misrepresents its services
22 is LifeLock.identity-protection.org. This website bears LifeLock's insignia and contains
23 no disclaimer that it is independent of LifeLock.

24 83. On this website, LifeLock touts its "proactive identity theft protection
25 services[.]" Importantly, unlike some others, LifeLock on this site represents it provides
26 its customers contemporaneous alerts of potential identity theft—regardless of whether the
27 customer has elected to receive the alert by phone, email, or text message.
28

1 **IV. LifeLock Breached Its Contractual Obligations.**

2 77. Through its advertising, website, and Service Terms, LifeLock promised
3 Plaintiffs and Class members that LifeLock would protect their identity by, among other
4 things, alerting them to address changes linked to their identity.

5 78. Plaintiffs and the Class members accepted LifeLock's offer and provided
6 consideration through payment of Membership Fees.

7 79. Plaintiffs and the Class members' contracts with LifeLock all contain the
8 following provisions:

9 These LifeLock Service Terms and Conditions (the "Service
10 Terms") are a legally binding agreement between LifeLock,
11 Inc. ("LifeLock," "we" "our" or "us") and you ("you," "your"
12 or "yours"), and describe the terms under which you agree to
13 use the LifeLock identity programs, including any applicable
14 Stolen Identity Insurance (the "Protection Programs"), credit
15 monitoring service (the "Credit Monitoring Service") and any
16 other service or product which may be made available to you
17 by us for which you have registered or enrolled or have been
18 registered or enrolled by an authorized third party (collectively
19 the "Services" and individually a "Service").

20 The Service Terms and any Services provided hereunder will
21 be governed by the laws of the State of Arizona, without
22 regard to any laws that would direct the choice of another
23 state's laws and, where applicable, will be governed by the
24 federal laws of the United States.

25 Accordingly, class-wide application of Arizona law is appropriate.

26 80. In the Service Terms, LifeLock itself acknowledges that its website
27 promises regarding its Membership Plans are incorporated into the Service Terms.

28 81. LifeLock breached its contract with Plaintiffs and the members of the Class
by: (1) failing to notify LifeLock Standard Members, and perhaps others, of address
changes, (2) failing to notify LifeLock Advantage and Ultimate Plus Members of address
changes as promised, and by (3) making material misrepresentations about LifeLock's
Services.

82. Over 4 million people paid between \$10.00 and \$30.00 per month for a
service LifeLock promised, but did not—and could not—provide. Because LifeLock
broke that promise, those who subscribed to LifeLock's products at worst were left

1 unprotected and suffered further harm, and at best were paying for a service that they were
2 not receiving.

3 83. Specifically, LifeLock promised to monitor the USPS's change-of-address
4 data, and other address-change data linked to the customer's identity, and provide timely
5 alerts when an address change was initiated for a LifeLock customer.

6 84. LifeLock does not directly purchase change-of-address data from the USPS
7 and lacks any means of providing anything close to a timely alert of an address change.

8 85. Furthermore, LifeLock altogether refused to provide those alerts, or did so
9 only sporadically, to members of LifeLock's Standard Plan and thus dishonored that
10 obligation to a whole segment of its customers.

11 86. And for those who purchased the more expensive LifeLock plans, LifeLock
12 provided nothing approximating timely notice of address changes. Indeed, LifeLock's
13 alerts could come weeks after someone initiated the address change, much too late to
14 make the alert a tool in preventing identity theft.

15 87. In sum, LifeLock fails to make good on its promises to its consumers. And
16 in exchange, over 4 million subscribers pay LifeLock up to \$30.00 a month, believing
17 they are protected when in fact they are getting nothing in return.

18 **FRAUDULENT CONCEALMENT AND TOLLING**

19 88. The applicable statutes of limitations are tolled by virtue of Defendant's
20 knowing and active concealment of the facts alleged above. Plaintiffs and Class members
21 were ignorant of the information essential to the pursuit of these claims, without any fault
22 or lack of diligence on their own part.

23 89. At the time this action was filed, Defendant was under a duty to disclose the
24 true, character, quality, and nature of LifeLock's services to Plaintiffs and the Class.
25 Defendant is therefore estopped to rely on any statute of limitations.

26 90. Defendant's fraudulent concealment is common to the Class.
27
28

CLASS ACTION ALLEGATIONS

1
2 91. Plaintiffs bring this action against LifeLock as a class action pursuant to
3 Federal Rules of Civil Procedure 23(a) and 23(b)(2) and (b)(3).

4 92. Plaintiffs seek certification of this action on behalf of the following class
5 (the “Class”): all persons in the United States who are or were, during January 21, 2016
6 through the resolution of this matter (the “Class Period”) subscribers of LifeLock’s fee-
7 based identity-theft protection services. Excluded from the Class are Defendant, any
8 parent, subsidiary, affiliate, or controlled person of Defendant, as well as the officers,
9 directors, agents, servants, or employees of Defendant and the immediate family members
10 of any such person. Also excluded is any judge who may preside over this cause of action.

11 93. The exact size of the Class, as herein identified and described, is not known,
12 but it is estimated to number in the millions. The Class is so numerous that joinder of
13 individual members herein is impracticable.

14 94. There are common questions of law and fact in the action that relate to and
15 affect the rights of each member of the Class and the relief sought is common to the entire
16 Class. In particular, the common questions of fact and law include:

- 17 (A) Whether Defendant provided change-of-address alerts to members of
18 its Standard Plan;
- 19 (B) Whether Defendant was capable of providing, as promised, change-
20 of-address alerts to members of any of its plans;
- 21 (C) Whether Defendant misrepresented, either expressly or by
22 implication, the true nature of its Bank and Credit Card Alerts;
- 23 (D) Whether Defendant misrepresented, either expressly or by
24 implication, the true nature of its services via statements made by
25 Affiliates;
- 26 (E) Whether Defendant misrepresented, either expressly or by
27 implication, the true nature of the benefits of its Million Dollar
28 Protection Package;

1 (F) Whether Arizona law applies to the putative Class; and

2 (G) Whether members of the Class have sustained damages, and, if so, in
3 what amount.

4 95. The claims of the Plaintiffs, who are representative of the Class herein, are
5 typical of the claims of the proposed Class, in that the claims of all members of the
6 proposed Class, including the Plaintiffs, depend on a showing of the acts of Defendant
7 giving rise to the right of Plaintiffs to the relief sought herein. There is no conflict
8 between the individually named Plaintiffs and other members of the proposed Class with
9 respect to this action or with respect to the claims for relief set forth herein.

10 96. The named Plaintiffs are the representative parties for the Class, and are able
11 to, and will fairly and adequately protect the interests of the Class. The attorneys for
12 Plaintiffs and the Class are experienced and capable in complex civil litigation, consumer
13 fraud litigation, and class actions.

14 97. The class action procedure is superior to all other available methods for the
15 fair and efficient adjudication of this controversy. This action would permit a large
16 number of injured persons to prosecute their common claims in a single forum
17 simultaneously, efficiently, and without unnecessary duplication of evidence and effort.
18 Class treatment also would permit the adjudication of claims by class members whose
19 claims are too small and complex to individually litigate against a large corporate
20 defendant.

21 ***COUNT I***
22 **Violation of the Arizona Consumer Fraud Act**

23 98. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

24 99. Defendant sold Plaintiffs and other Class Members “merchandise” as that
25 term is defined by A.R.S. § 44-1521, in the form of services, including alleged identity-
26 theft protection services and all other services offered under the various plans.

27 100. Section 44-1522 of the Arizona Consumer Fraud Act provides:

28 The act, use or employment by any person of any deception, deceptive or
unfair act or practice, fraud, false pretense, false promise, misrepresentation,

1 or concealment, suppression or omission of any material fact with intent that
2 others rely on such concealment, suppression or omission, in connection
3 with the sale or advertisement of any merchandise whether or not any person
4 has in fact been misled, deceived or damaged thereby.

5 *See* A.R.S. § 44-1522(A).

6 101. LifeLock used deception, used a deceptive act or practice, and fraudulently
7 omitted or concealed material facts in connection with the sale or advertisement of that
8 merchandise in violation of A.R.S. § 44-1522(A).

9 102. LifeLock's acts and omissions constitute material misrepresentations and
10 concealments in connection with the sale or advertisement of its services in violation of
11 the Arizona Consumer Fraud Act, A.R.S. § 44-1522(A).

12 103. Specifically, LifeLock used false, deceptive, and misleading statements,
13 concerning the scope and effectiveness of its services; its ability to monitor USPS data for
14 address changes; that it provided members of its Standard Plan change-of-address alerts;
15 and that it provided such alerts as promised to members of all its plans.

16 104. Likewise, LifeLock's advertisements and website were misleading, false,
17 and/or deceptive regarding the efficacy of LifeLock's technology and safeguards.

18 105. LifeLock further omitted and/or concealed material facts. For example,
19 LifeLock concealed the fact that it had no means of monitoring changes in address on
20 anything approaching a continuous basis—and that any alerts of address changes would
21 come weeks or a month later.

22 106. The concealed facts are material in that they are logically related to the
23 transactions at issue and rationally significant to the parties in view of the nature and
24 circumstances of those transactions.

25 107. As a result of LifeLock's misrepresentations and omissions, LifeLock's
26 members paid substantial fees, were injured and sustained damages in an amount to be
27 proven at trial. These damages include, at a minimum, payments of monthly charges for
28 services that were not as represented, and which in many cases LifeLock had no intention
of delivering.

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

COUNT II
Breach Of Contract

108. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

109. In its plans and agreements with Plaintiffs and Class members, LifeLock agreed to provide Plaintiffs and the members of the Class Membership Plans and protections as advertised and promised.

110. As set forth herein, LifeLock breached its contracts with Plaintiffs and the members of the Class by failing to provide the benefits and/or protections as promised.

111. As a direct and proximate result of Defendant's breach, Plaintiffs and the Class are entitled to all damages arising from the breach of contract.

COUNT III
Unjust Enrichment

112. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

113. Plaintiffs and the Class conferred monetary benefits upon the Defendant by paying Membership Fees for the promised identity theft protections and services.

114. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class members.

115. Although LifeLock received earnings and benefits from the sale of its Membership Plans and the collection of Membership Fees from Plaintiffs and Class members, LifeLock retained these revenues under conditions that would constitute an unjust enrichment of those revenues.

116. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class members because Defendant failed to provide the promised services and misrepresented its ability to provide those services.

117. As a direct and proximate result of Defendant's actions, Plaintiffs and the Class are entitled to restitution on the full amount by which the Defendant has been unjustly enriched and should be required to disgorge same to Plaintiffs and the Class.

COUNT IV
Declaratory Judgment

1
2 118. Plaintiffs hereby repeat and reallege all preceding paragraphs contained
3 herein.

4 119. An actual case and controversy within the meaning of the Federal
5 Declaratory Judgment Act, 28 U.S.C. §§ 2201 and 2202, which may be adjudicated by
6 this Court exists between Plaintiffs and proposed class members, and the Defendant.

7 120. Plaintiffs and all members of the proposed class have, had, or were
8 subscribers of one of Defendant’s fee-based Membership Plans. Defendant’s Terms and
9 Conditions provide that its insureds are treated consistent with the requirements of the
10 laws and regulations of Arizona. Thus, per the governing contract, Arizona law controls
11 how the Defendant’s customers must be treated by Defendant.

12 121. At the same time, the relationship between Defendant and its customers was
13 subject to the FTC Preliminary Injunction entered between Defendant and the FTC in
14 2010, as amended in 2015, which specifically enjoins LifeLock from misrepresenting,
15 expressly or by implication, “the means, methods, procedures, effects, effectiveness,
16 coverage, or scope” of LifeLock’s services.

17 122. Defendant, as a general policy and business practice, represented or created
18 the impression that LifeLock’s Membership Plans provide: (a) protection from fraud or
19 unauthorized account charges or “peace of mind”; (b) a solution to financial security; (c)
20 live member support 24/7/365 and real-time “alerts” of any threat of identity theft; and
21 contemporaneous monitoring of the United States Postal Service’s change-of-address
22 data.

23 123. Accordingly, Defendant has violated, and continues to violate, Arizona law
24 and the FTC Preliminary Injunction and Plaintiffs are entitled to declaratory relief.

RELIEF

25
26 WHEREFORE, Plaintiffs, individually and on behalf of all others similarly
27 situated, respectfully request that this Court:
28

- 1 a) determine that this action may be maintained as a class action under Rule 23
2 of the Federal Rules of Civil Procedure, that Plaintiffs are proper class
3 representatives, and approve Plaintiffs' Counsel as counsel for the Class;
4 b) enter an order demanding that Defendant pay monetary damages to the
5 Plaintiffs, and all proposed Class members;
6 c) enter an order declaring that Defendant's actions are unlawful; and
7 d) grant such other legal and equitable relief as the Court may deem
8 appropriate, including costs and attorneys' fees pursuant to A.R.S. § 12-
9 341.01.

10 **JURY DEMAND**

11 Plaintiffs and the Class members hereby request a trial by jury.

12 RESPECTFULLY SUBMITTED this 30th day of March 2018.

13
14 GALLAGHER & KENNEDY, P.A.

15 By: s/ Paul L. Stoller

16 Paul L. Stoller
17 Lincoln Combs
2575 East Camelback Road
Phoenix, Arizona 85016-9225

18 CARNEY BATES & PULLIAM, PLLC
19 Randall K. Pulliam
E. Lee Lowther III
20 519 W. 7th St.
Little Rock, AR 72201
21 Telephone: (501) 312-8500
Facsimile: (501) 312-8505

22 COHEN MALAD, LLP
23 Irwin B. Levin
Richard E. Shevitz
24 Vess A. Miller
Lynn A. Toops
25 One Indiana Square, Suite 1400
Indianapolis, IN 46204
26 Telephone: (317) 636-6481
Facsimile: (317) 636-2593

27 *Attorneys for Plaintiffs*

28

UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

Civil Cover Sheet

This automated JS-44 conforms generally to the manual JS-44 approved by the Judicial Conference of the United States in September 1974. The data is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. The information contained herein neither replaces nor supplements the filing and service of pleadings or other papers as required by law. This form is authorized for use only in the District of Arizona.

The completed cover sheet must be printed directly to PDF and filed as an attachment to the Complaint or Notice of Removal.

Plaintiff(s): Joe Weingarten ; Darrell Hunter
County of Residence: Outside the State of Arizona
County Where Claim For Relief Arose: Outside the State of Arizona

Defendant(s): LifeLock, Inc.
County of Residence: Maricopa

Plaintiff's Atty(s):
**Paul L. Stoller
Gallagher & Kennedy PA
2575 E. Camelback Rd.
Phoenix, Arizona 85016
602-530-8000**

Defendant's Atty(s):

II. Basis of Jurisdiction: **4. Diversity (complete item III)**

III. Citizenship of Principal Parties (Diversity Cases Only)

Plaintiff:- **2 Citizen of Another State**
Defendant:- **1 Citizen of This State**

IV. Origin : **1. Original Proceeding**

V. Nature of Suit: **190 Other Contract**

VI. Cause of Action: **28 USC 1332(d)**

VII. Requested in Complaint

Class Action: **Yes**
Dollar Demand:
Jury Demand: **Yes**

VIII. This case is not related to another case.

Signature: s/ Paul L. Stoller

Date: 3/30/18

If any of this information is incorrect, please go back to the Civil Cover Sheet Input form using the *Back* button in your browser and change it. Once correct, save this form as a PDF and include it as an attachment to your case opening documents.

Revised: 01/2014