

COPY

[EXEMPT FROM FILING FEES
UNDER GOVT. CODE SEC. 6103]

1 KAMALA D. HARRIS
Attorney General of California
2 ROBERT MORGESTER
Senior Assistant Attorney General
3 ADAM MILLER
Supervising Deputy Attorney General
4 State Bar No. 168254
455 Golden Gate Avenue, Suite 11000
5 San Francisco, CA 94102-7004
Telephone: (415) 703-5551
6 Fax: (415) 703-1234
E-mail: Adam.Miller@doj.ca.gov

ENDORSED
FILED
ALAMEDA COUNTY

AUG 29 2013

CLERK OF THE SUPERIOR COURT
By _____

Deputy
PILIPINO TUNGOHAN

7 *Attorneys for Plaintiff*
8 THE PEOPLE OF THE STATE OF CALIFORNIA

10 SUPERIOR COURT OF THE STATE OF CALIFORNIA

11 COUNTY OF ALAMEDA

AG 13693591

14 **THE PEOPLE OF THE STATE OF
15 CALIFORNIA,**

16 Plaintiff,

17 v.

18 **CITIBANK, N.A.,**

19 Defendant.
20

Case No.

**COMPLAINT FOR INJUNCTION, CIVIL
PENALTIES AND OTHER EQUITABLE
RELIEF FOR VIOLATIONS OF
BUSINESS AND PROFESSIONS CODE
SECTION 17200 (UNFAIR
COMPETITION LAW)**

21
22 Plaintiff, the People of the State of California, by and through Kamala D. Harris, Attorney
23 General of the State of California, alleges the following on information and belief:

24 **DEFENDANT AND VENUE**

25 1. Defendant Citibank, N.A., ("Citibank") is a national bank with its head office
26 located at 701 East 60th Street North, Sioux Falls, South Dakota 57104.

27 2. Citibank is engaged in the business of banking. Citibank provides banking
28 services to California residents, including checking and savings accounts, credit card and debit

1 card accounts, and numerous bank branches located within the State of California. Citibank also
2 provides a Web site located at <https://www.accountonline.com> ("Account Online") through which
3 Citibank provides its credit card and debit card customers with access to information relating to
4 their accounts.

5 3. Citibank at all times mentioned herein has transacted business in the County of
6 Alameda and elsewhere within the State of California. The violations of law described herein
7 occurred in the County of Alameda and elsewhere in the State of California.

8 **DEFENDANTS' BUSINESS ACTS AND PRACTICES**

9 4. On or about May 10, 2011, Citibank discovered that its Account Online service
10 had been breached by a computer hacking exploit. The breach took advantage of a known
11 technical vulnerability that had been implemented by Citibank on Account Online in or about
12 July of 2008. The vulnerability permitted the unknown computer hacker(s) to access multiple
13 user accounts on Account Online by logging in with a known account number and password, then
14 modify a few characters of a query string that appeared in the resulting Web browser's Universal
15 Resource Locator ("URL") bar in order to access additional accounts.

16 5. A very simple example of such a query string modification hack is as follows: If
17 the hacker(s) properly logged into account number 12345, the URL might appear in the Web
18 browser's URL as something like "https://www.citibank.com/user/?CARD_NUMBER=12345."
19 The hacker(s) could then merely modify a few characters on the URL to something like
20 "https://www.citibank.com/user/?CARD_NUMBER=12346" and would then have access to
21 account number 12346, without having to independently authenticate or log in. The hacker(s)
22 then used a simple script that automatically scraped all the account information, saved it, and then
23 changed the numbers in the URL and repeated the process.

24 6. Citibank did not permanently fix this vulnerability until on or about May 27, 2011,
25 nearly three years after the vulnerability had been implemented on Account Online. Citibank
26 started notifying its affected customers about the breach on or about June 3, 2011, and did not
27 complete its notifications until on or about June 11, 2011, over one month after the breach was
28 detected by Citibank.

1 7. Through this preventable exploit, account information for over 360,000 Citibank
2 customers, including approximately 80,454 California citizens, was accessed and/or obtained by
3 the hacker(s). The account information included customer names, street addresses, email
4 addresses, phone numbers, and credit card account numbers.

5 8. On its Web site Citibank posts a privacy policy that states that Citibank protects
6 customers' personal "information by maintaining physical, electronic, and procedural safeguards
7 that meet applicable law."¹

8 9. Under the California Online Privacy Protection Act, California Business and
9 Professions Code sections 22575-22578 ("CalOPPA"), an operator of a commercial Web site or
10 online service that collects personally identifiable information from individual consumers
11 residing in California is in violation of CalOPPA if it fails to comply with the provisions of its
12 posted privacy policy, either (a) knowingly and willfully; or (b) negligently and materially.

13 10. Under California Civil Code section 1798.82, business that own or license
14 computerized data must disclose to consumers "in the most expedient time possible and without
15 unreasonable delay" data breach incidents concerning consumers' specified personal information.

16 11. Under the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq, "GLBA"), Citibank
17 is a "Financial Institution" that must take sufficient steps to protect the privacy and security of
18 customers' personally identifiable financial information. As a national bank, Citibank is
19 regulated by the Office of the Comptroller of the Currency ("OCC"). OCC standards for
20 information security are set forth in Appendix B of 12 CFR Part 30, entitled "Interagency
21 Guidelines Establishing Information Security Standards" (the "OCC Guidelines"). In particular,
22 Section III.C.1 ("Manage and Control Risk") of the OCC Guidelines provides that each bank
23 shall "[d]esign its information security program to control the identified risks, commensurate with
24 the sensitivity of the information as well as the complexity and scope of the bank's activities," and,
25 where appropriate, adopt "[a]ccess controls on customer information systems, including controls
26 to authenticate and permit access only to authorized individuals ..."

27 ¹ Citibank's Web site Privacy Policy was last modified July 31, 2011. (See
28 <https://online.citibank.com/JRS/portal/template.do?ID=Privacy>, accessed August 12, 2013.)

1 FIRST CAUSE OF ACTION

2 VIOLATIONS OF BUSINESS AND PROFESSIONS CODE SECTION 17200

3 (UNFAIR COMPETITION)

4 12. Plaintiff realleges Paragraphs 1 through 11 and incorporates these Paragraphs by
5 reference as though they were fully set forth in this cause of action.

6 13. Citibank engaged in unlawful, unfair or fraudulent business acts or practices
7 within the meaning of Business and Professions Code section 17200 et seq., including, but not
8 limited to, the following:

9 (a) Citibank violated CalOPPA, and in particular, California Business and
10 Professions Code section 22576, in that Citibank failed to comply with the provisions of its
11 posted Web site privacy policy, by failing to maintain physical, electronic or procedural
12 safeguards for Account Online that meet applicable law. In particular, in violation of the GLBA
13 and the OCC Guidelines, Citibank as a "Financial Institution" did not take sufficient steps to
14 protect the privacy and security of customers' personally identifiable financial information, by
15 failing to adopt sufficient "[a]ccess controls on customer information systems, including controls
16 to authenticate and permit access only to authorized individuals" and failing to prevent the
17 computer hacking exploit described in this Complaint. This violation was either (1) knowing and
18 willful; or (2) negligent and material, because Citibank had installed and knew, or should have
19 known, about the technical vulnerability within Account Online in or about July of 2008, and the
20 known technical vulnerability lead to unauthorized access to customers' personal data.

21 (b) Citibank violated California Civil Code section 1798.82, subdivision (a),
22 by failing to expediently notify its California resident customers of the breach of the security of
23 Account Online data, and unauthorized acquisition of their unencrypted personal information.

24 (c) Citibank violated California Civil Code section 1798.82, subdivision (b),
25 by not immediately notifying the owners or licensees of computerized data of the breach of the
26 security of Account Online data, in that their unencrypted personal information was or reasonably
27 believed to have been acquired by an unauthorized person.

28 //

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

1. That under California Business and Professions Code section 17203, Citibank, its successors, agents, representatives, employees, and all persons who act in concert with Citibank be permanently enjoined from committing any acts of unfair competition, including the violations alleged in the First Cause of Action.

2. That under California Business and Professions Code section 17206, Citibank be ordered to pay Two Thousand Five Hundred Dollars (\$2,500) for each violation of California Business and Professions Code section 17200 by Citibank, as proved at trial.

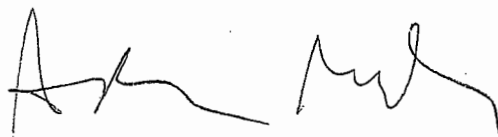
3. That Plaintiff recovers its cost of suit herein, including costs of investigation.

4. For such other and further relief as the Court may deem just and proper.

Dated: August 28, 2013

Respectfully Submitted,

KAMALA D. HARRIS
Attorney General of California
ROBERT MORGESTER
Senior Assistant Attorney General



ADAM MILLER
Supervising Deputy Attorney General
Attorneys for Plaintiff
THE PEOPLE OF THE STATE OF CALIFORNIA

SF2012803857
20689839.doc

DECLARATION OF SERVICE BY U.S. MAIL

Case Name: People v. Citibank, N.A.
No.: Alameda County Superior Court

I declare:

I am employed in the Office of the Attorney General, which is the office of a member of the California State Bar, at which member's direction this service is made. I am 18 years of age or older and not a party to this matter. I am familiar with the business practice at the Office of the Attorney General for collection and processing of correspondence for mailing with the United States Postal Service. In accordance with that practice, correspondence placed in the internal mail collection system at the Office of the Attorney General is deposited with the United States Postal Service with postage thereon fully prepaid that same day in the ordinary course of business.

On August 28, 2013, I served the attached **COMPLAINT FOR INJUNCTION, CIVIL PENALTIES AND OTHER EQUITABLE RELIEF FOR VIOLATIONS OF BUSINESS AND PROFESSIONS CODE SECTION 17200 (UNFAIR COMPETITION LAW)** by placing a true copy thereof enclosed in a sealed envelope in the internal mail collection system at the Office of the Attorney General at 455 Golden Gate Avenue, Suite 11000, San Francisco, CA 94102-7004, addressed as follows:

William L. Stern
Morrison & Foerster
425 Market Street
San Francisco, CA 94105

I declare under penalty of perjury under the laws of the State of California the foregoing is true and correct and that this declaration was executed on August 28, 2013, at San Francisco, California.

Brenda Zuniga
Declarant



Signature