



OFFICE OF THE ATTORNEY GENERAL
STATE OF ILLINOIS

Lisa Madigan
ATTORNEY GENERAL

January 8, 2015

Ms. Zoe Strickland
Managing Director
Global Chief Privacy Officer
JPMorgan Chase & Co.
237 Park Avenue, 7th Floor
New York, NY 10017-3140

SENT VIA: E-Mail & First Class Mail

Ms. Lisa J. Sotto
Partner
Hunton & Williams LLP
200 Park Avenue
New York, NY 10166

Mr. Benjamin A. Powell
Partner
WilmerHale
1875 Pennsylvania Avenue, NW
Washington, DC 20006

Re: JPMorgan Chase Breach

Dear Ms. Strickland:

Our offices are leading a group of Investigating States that presently includes the Offices of Attorneys General for the following States: [REDACTED], Connecticut, [REDACTED], Illinois, [REDACTED], [REDACTED], [REDACTED], [REDACTED], and [REDACTED] (the "Multistate"). To the extent other States join the Multistate, we will advise you of such.

[REDACTED]



The Multistate is writing to express its concern and request additional information regarding the recent data breach at JPMorgan Chase ("JPMC"), which reportedly affected seventy-six (76) million household accounts and seven (7) million small-business accounts nationwide. From our discussions with JPMC thus far, we understand that this incident involved the unauthorized access to certain customer information maintained by JPMC, including names, addresses, phone numbers, email addresses, and "internal JPMC information relating to such users." This incident raises concerns about the security of our States' residents' private information in the hands of JPMC. Further, critical facts about the intrusion remain unclear, including details concerning the cause of the breach and the nature of any procedures adopted or contemplated to prevent future breaches.

The Multistate therefore requests that JPMC provide it with more detailed information pertaining to the nature and status of this incident. As such, please provide information responsive to the following questions by January 23, 2015. While some of this information may presently be unknown or under investigation, it is imperative to the protection of our States' residents that we better understand the circumstances of this breach as they are known by JPMC presently.

1. Please describe the facts and circumstances of the breach, including a complete timeline of events leading up to the discovery of the breach, any vulnerability exploited in connection with the breach, and JPMC's efforts to investigate and mitigate thereafter.
2. Please identify the information about consumers maintained by JPMC, including, but not limited to, the categories of information and the specific data points that comprise each category.
3. Please identify the information about consumers subject to the breach, including, but not limited to, the categories of information and the specific data points that comprise each category.
4. Please describe in detail the basis for JPMC's statement that there is "no evidence that account numbers, passwords, user IDs, date of birth or Social Security numbers were compromised during this attack." Please state whether JPMC's investigation has revealed any information inconsistent with such statement.
5. For each State participating in the Multistate, please provide the number of consumers affected by the breach.
6. Please identify whether JPMC is aware of any fraudulent activity regarding any compromised information, including, but not limited to, unauthorized account access and/or charges.
7. Please describe the technological, administrative and physical safeguards that were in place to protect the information compromised in this breach from unauthorized access or acquisition. As part of your response, please provide a copy of any policies and procedures relating to:

- a. login credentials, including passwords, needed to access servers that contain sensitive data or consumer information and any required periodic changes of such passwords;
 - b. use of two-factor authentication for access to servers that contain sensitive data or consumer information;
 - c. server and software upgrades, including application of software patches; and
 - d. internet security, including security requirements for internet-connected servers.
8. Please identify any additional safeguards, both adopted and contemplated, that have been or are to be taken in an effort to prevent future breaches of consumer information.
 9. Please provide a copy of any and all compliance materials, both public and non-public, regarding compliance with the Gramm-Leach-Bliley, Financial Privacy and Safeguards Rule.
 10. Please provide a copy of JPMC's Privacy Policy(ies), both current and as made available to consumers during the ten (10) years prior to this breach.
 11. Please provide a copy of any internal or third party investigative report or audit performed by or for JPMC relative to this breach.

The information requested herein should be sent to:

Matthew W. Van Hise
Consumer Privacy Counsel
Assistant Attorney General
Consumer Fraud Bureau
Illinois Attorney General's Office
500 South Second Street
Springfield, IL 62706
(217) 782-4436
mvanhise@atg.state.il.us

Matthew Fitzsimmons
Chair, Privacy Task Force
Assistant Attorney General
Office of the Attorney General
110 Sherman Street
Hartford, Connecticut 06105
(860) 808-5400
Matthew.Fitzsimmons@ct.gov

On behalf of the Multistate, we appreciate your anticipated cooperation and look forward to hearing from you.

