

# BROWN RAYSMAN

BROWN RAYSMAN MILLSTEIN FELDER & STEINER LLP

MAY 26 2006

Kristen J. Mathews  
(212) 895-2327  
kmathews@brownraysman.com

May 24, 2006

Consumer Protection Division  
North Carolina Department of Justice  
P.O. Box 629  
Raleigh, NC 27602

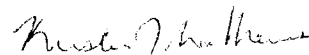
Dear To Whom it May Concern:

I am writing to you on behalf of my client, Mortgage Lenders Network USA, Inc., pursuant to the "Identity Theft Protection Act" (North Carolina General Statutes § 75-65(e)). On or about May 5, 2006, MLN became aware that a former employee of MLN may have compromised, or intended to compromise, certain sensitive consumer data to which he had access in connection with his employment. MLN took action promptly by discontinuing all access by the individual to MLN computer systems, files and data, and by notifying police authorities, in particular the Middletown, CT police department. On May 20, 2006, pursuant to a police investigation, MLN became aware that this former employee had files in his possession that were the property of MLN, and that contained sensitive customer information. MLN is cooperating with the authorities in an investigation into exactly what information was contained in the files.

While it does appear that this individual compromised certain personal information relating to MLN customers, there is no evidence at this time that there was any further dissemination or use of such data by this individual. However, it is possible that social security numbers could be subject to unauthorized use, as well as other information located in our customers' accounts such as name, mailing address, loan numbers and loan types. (Credit card, debit card and other financial account numbers would not have been subject to compromise.)

At this time MLN believes that there are approximately 231,000 individual account holders whose sensitive personal information was subject to the compromise, and it is possible that some of them are North Carolina residents, although the exact number of North Carolina residents, if any, has not yet been determined. MLN has sent, or plans to send, notice letters to each of the account holders, a copy of which is attached hereto. If you have any questions, please do not hesitate to contact me.

Sincerely,



Kristen J. Mathews

Dear Valued Customer,

I am writing you to let you know about a recent incident in which a former employee threatened the security of certain Mortgage Lenders Network USA, Inc. ("MLN") data.

On or about May 5, 2006, MLN became aware that a former employee may have compromised, or intended to compromise, certain sensitive consumer data to which he had access in connection with his employment. MLN took action promptly by discontinuing all access by the individual to MLN computer systems, files and data, and by notifying police authorities. On May 20, 2006, pursuant to a police investigation, MLN became aware that this former employee had files in his possession that were the property of MLN, and that contained sensitive customer information. MLN is cooperating with the authorities in an investigation into exactly what information was contained in the files.

While it does appear that this individual compromised certain personal information relating to our customers, there is no evidence at this time that there was any further dissemination or use of such data by this individual. However, it is possible that your social security number could be subject to unauthorized use, as well as other information located in your account such as your name, mailing address, loan numbers and loan types. (Your credit card, debit card and other financial account numbers would not have been subject to compromise.)

What should you do?

- Since your sensitive personal information has been subject to compromise, there are a few things you may want to do:
  - **You should periodically request a free credit report to ensure credit accounts have not been activated without your knowledge.** Every consumer, whether or not their data has been involved in a security breach, can receive one free report every twelve months from each of the three national credit bureaus listed below. In fact, it is a good practice for all consumers to order a free credit report from one of the three credit bureaus every four months, in order to continually monitor your accounts every year. To order your free credit report, contact one of the three major credit bureaus at the numbers provided below.
  - **You may also wish to take the added precaution of placing a fraud alert on your credit file.** A fraud alert tells creditors to contact you before they open any new credit accounts or change your existing accounts. To place a fraud alert on your credit file, contact one of the three national credit bureaus at the numbers provided below. This will let you automatically place fraud alerts and order your credit report from all three credit bureaus at once. If you decide to place a fraud alert on your credit file, you should be aware that:
    - (i) you may be asked to provide proof of identification when applying for instant credit, and in some cases your ability to receive instant credit may be limited,
    - (ii) creditors may contact you by phone at the number you designate before opening a new account for you,
    - (iii) a fraud alert should not interfere with the daily use of credit cards or banking or credit accounts, and
    - (iv) a fraud alert will expire, usually in 90 days, so you will need to renew it by calling the credit bureau you initiated it with, using the confirmation number you were given when you initiated (or subsequently renewed) the fraud alert.
  - In some states, you have the right to put a "credit freeze" on your credit file, so that no new credit can be opened under your credit file.

- **Once you receive your credit reports, check them carefully for unusual activity.** If you see any accounts you did not open or incorrect personal information, call the credit bureau(s) or your local law enforcement agency to file a report of identity theft. You should get a copy of the police report, and you may need to provide copies to creditors to clear up your records. Also, please notify us of any fraudulent activity that you discover in your credit file.
- **Even if you do not find suspicious activity on your initial credit reports, it is recommended that you check your credit reports periodically.** Victim information is sometimes held for use or shared among a group of thieves at different times. Remaining vigilant and checking your credit reports periodically over the next 12 to 24 months can help you spot problems and address them quickly.
  - Equifax (800) 525-6285 [www.equifax.com](http://www.equifax.com)
  - Experian (888) 397-3742 [www.experian.com](http://www.experian.com)
  - Trans Union (800) 680-7289 [www.transunion.com](http://www.transunion.com)

Because the investigation of this incident is ongoing, we do not have all of the details at this time. We will continue to investigate this matter thoroughly and take all necessary and immediate steps to reduce the chance of any future incidents.

**Other than in the form of a written letter, Mortgage Lenders Network will not initiate contact with you about this incident, and will not ask you to confirm any sensitive personal information, such as your Social Security number. If you do happen to receive a contact with such a request, it is not from Mortgage Lenders Network, and you should not provide any such information.**

MLN regards the privacy of consumer information with the utmost of importance. To that end, MLN has numerous security measures in place to safeguard MLN accounts. Further, MLN continues to implement additional security measures in order to meet the demands of the today's computer based society.

If there is anything we can do to assist you further, please feel free to call us at **1-800-308-8965** or contact us at the information provided below.

We truly regret any inconvenience.

Sincerely,

***MORTGAGE LENDERS NETWORK USA, INC.***

---

**Mortgage Lenders Network USA, Inc.  
Legal Department  
213 Court Street  
Middletown, CT 06457**

**[www.MLNUSA.com](http://www.MLNUSA.com)**

# BROWN RAYSMAN

BROWN RAYSMAN MILLSTEIN FELDER & STEINER LLP

Kristen J. Mathews  
(212) 895-2327  
kmathews@brownraysman.com

June 29, 2006

Ms. Kim D'Arruda  
Assistant Attorney General  
Consumer Protection/Antitrust Division  
North Carolina Department of Justice  
P.O. Box 629  
Raleigh, NC 27602

Dear Ms. D'Arruda:

Thank you for your letter, dated June 9, 2006, regarding our notification of the security incident involving Mortgage Lenders Network U.S.A, Inc.'s ("MLN") data. In response to your specific requests in such letter for further information regarding the security incident, we are providing the information below.

(1) Were the files possessed by the former employee, and any other data that may have been compromised, password protected or somehow encrypted?

The information that was possessed by the former employee of MLN was, in fact, password protected, but not encrypted. Nonetheless, encryption would not have been effective against access by the former employee, who, at the time of his access, was employed by MLN and possessed an authorized password, which allowed him to access the data as part of his employment.

(2) Describe any measures taken to prevent a similar security breach from occurring in the future.

Since MLN became aware that the incident had occurred, the risk management team at MLN has been working diligently to develop a comprehensive report on the incident, which will include additional protective and security measures to be implemented to prevent a similar security incident from occurring again. We will be able to provide you with a more detailed response regarding such preventative measures as soon as the report has been completed.

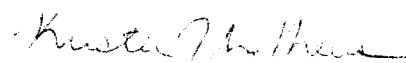
BRMF51 925633v2

(3) What is the number of North Carolina residents whose personal information was subject to the breach?

Sensitive personal information of approximately 5,424 North Carolina residents was potentially subjected to the breach.

If you have any further questions, please do not hesitate to contact me.

Sincerely,

A handwritten signature in cursive script, appearing to read "Kristen J. Mathews".

Kristen J. Mathews