



September 8, 2009

Kelly A. Ayotte
State of New Hampshire: Attorney General
33 Capitol St
Concord, NH 03301-6310

Dear Attorney General Ayotte,

This letter serves as notification by Massachusetts Mutual Life Insurance Company ("MassMutual") that the personal information of a resident of New Hampshire has been acquired by an unauthorized third party.

On August 3, 2009, MassMutual was advised, verbally and in writing, by Postal Inspector James Morrison of the U.S. Postal Inspection Service ("Service") that during the course of an identity theft investigation, the Service discovered documents containing the personal information of certain MassMutual customers in an envelope bearing MassMutual's logo. The Service advised that they had reason to believe that at least some of this personal information had been used for fraudulent purposes. On August 5, 2009, the Service requested, verbally and in writing, that MassMutual delay notification to impacted individuals in order to prevent a compromise of the Service's investigation.

The documents recovered by the Service appear to be "screen prints" from one of MassMutual's administrative platforms and such documents contained, among other things, individual customer: (i) first and last name; (ii) address, (iii) Social Security number; and (iv) what appear to be financial account number(s). Each screen print also contained a unique identifier for the MassMutual employee who had access to the system at the time the document was printed. All reviewed "screen prints" appear to have been generated by one individual, who left MassMutual's employ in March of 2008.

Based on information currently available, seventy three (73) MassMutual customers have been impacted by this incident, one of which is a resident of New Hampshire. The impacted New Hampshire resident will receive a breach notification, which will be provided by first class mail. Such notification will be sent to impacted individuals contemporaneously with this notification to the Office of the Attorney General and the New Hampshire Insurance Department.

MassMutual has fully cooperated with the Service's investigation into this incident and continues to cooperate and share information. MassMutual has undertaken an internal review of the incident and has determined that no fraudulent or suspicious transactions appear to have occurred with respect to the accounts of the customers whose information was compromised by this incident. MassMutual has placed internal warning codes and security measures on these

Kelly A. Ayotte
State of New Hampshire: Attorney General
September 8, 2009
Page 2

accounts in the event that any transactions are requested in these accounts. MassMutual intends to offer the impacted customers reimbursement for costs related to fraud monitoring programs and credit reports.

In the event that you have any questions, or if you need additional information, please do not hesitate to contact me. I may be reached at [REDACTED] or via email at [REDACTED].

Sincerely,

A handwritten signature in blue ink, appearing to read 'CJM', followed by a long horizontal flourish.

Christopher J. Markowski
Counsel

Enc.

verify the accuracy of personal information, such as home address and social security number. If you see anything that you do not understand, you can call the credit agency at the telephone number on the report.

If you find suspicious activity on your credit report, you should contact your local police or sheriff's office and file a police report for identity theft. In these circumstances, you may need copies of the police report to provide to creditors to clear up your records.

Even if you do not find signs of fraud on your reports, you may want to check your credit report every three months for the next year. We will reimburse you for the cost of obtaining those credit reports or for the cost of a reasonable credit monitoring services, such as those provided by the credit reporting agencies identified above.

You should closely examine your credit card, debit card, and bank statements immediately after you receive them to determine whether there are any unauthorized transactions and promptly notify any suspicious activity or suspected identity theft to law enforcement, or your state's Attorney General, and/or the Federal Trade Commission.

If at any time you are concerned about identify theft, you can place a fraud alert on your credit file at no cost to you. A fraud alert requires that creditors contact you before opening new accounts. By calling any one of the above credit reporting agencies, you can automatically place a fraud alert with all three reporting agencies for 90 days or seven years by providing them with certain required documentation and order your credit report from all three.

For more information on identity theft, you can contact the Federal Trade Commission at www.ftc.gov, at 1-877-438-4338, or at Consumer Response Center, F.T.C., 600 Pennsylvania Avenue, NW, Washington, DC 20580.

We sincerely regret any inconvenience caused by this incident, and we encourage you to contact Jeffrey James in our Customer Relations area at 1-800-895-6277 ext. 46166 if you have any questions.

Sincerely,

Diana Perlman
Assistant Vice President