

GMAC
Insurance

RECEIVED
OFF OF THE ATTY GENERAL

2008 APR -1 P 3:30

April 2, 2008

Office of Attorney General
Attn: Hugh Williams
200 Saint Paul Place
Baltimore, Maryland 21202

Dear Mr. Williams:

On March 25, 2008, GMAC Insurance (GMACI) was advised that a laptop computer belonging to a business partner's employee, along with other items of value, was stolen in a home burglary on March 23, 2008. The incident was reported to local Ohio law enforcement authorities and an investigation is underway.

Over the course of their investigation into the incident, which concluded March 29, 2008, our business partner advised us that the laptop contained two files of GMACI employee information that were unencrypted. One file contained GMACI's internal ID for each employee along with their social security numbers. The other file contained the internal IDs along with the employees' names. No other personally identifying information was on the files. We are notifying you of this incident in compliance with your state's security breach law.

In addition, we have reported this incident to Transunion, Equifax and Experian.

As our business partner's investigation continued, we kept our active employees advised of the situation via intra-company email. Copies of those communications are attached for your records. And, although we believe the potential for harm to our employees is remote because of the circumstances of the theft, GMACI is sending a written notice to those employees whose information was on the files. We expect to complete mailing the notification letter to approximately 2,802 individuals by April 4, 2008. The files involved indicate that 6 GMACI employees residing in the state of Maryland will receive the written notice.

For your records, I have attached the following:

1. First intra-company email to existing employees notifying them of the initial incident;
2. Second intra-company email to existing employees advising them of further developments;
3. Third intra-company email to existing employees advising them of the discovery of the second file containing unencrypted GMACI employee information;

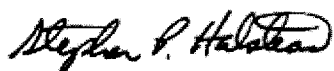
GMAC

Insurance

4. Script being used to notify former GMACI employees and existing employees, on leave of absence, of the incident;
5. Copy of written notice being mailed to impacted individuals in Maryland; and
6. Question and Answer document created to respond to employee inquiries.

Please do not hesitate to contact me at 336-770-2862 if you have questions.

Sincerely,



Stephen P. Halstead
Assistant General Counsel
GMAC Insurance

CONTENT OF NOTIFICATION LETTER BEING MAILED TO MARYLAND RESIDENTS
IMPACTED-6 RESIDENTS

Date

Employee Name

Address

Address

Dear xx:

On March 25, 2008, we were advised by a business partner that a laptop computer, belonging to one of their employees, was stolen in a home burglary on March 23, 2008. The business partner is our systems support vendor for our human resources/payroll databases.

The incident has been reported to law enforcement authorities and an investigation is underway. Please be assured that we are taking this matter seriously, and we are working with our business partner and the authorities to further investigate this matter. As you may be aware through security information posted to our intranet and shared with all employees, privacy is an important issue to us and we wanted to share this information with you as soon as possible.

The laptop contained two unencrypted files with GMACI Personal Lines employee information. One file contained employees' name and GMACI-PL user (*Pointsec*) ID sign on. The second file contained employees' GMACI-PL user (*Pointsec*) ID sign on and social security number. There was no other personally identifying information in the files. We have been informed by the business partner that the laptop was password protected. For further clarification, the files did not contain any salary or paycheck amounts.

The business partner is undertaking a thorough review of their internal security policies and will be implementing additional technical and administrative measures. In addition, this incident has accelerated the vendor's encryption plans, and GMAC Insurance will be monitoring to ensure that they protect our personal information to our own high standards and comply with our security policy.

Although we believe the chance of someone using this information to harm you is extremely remote because of the circumstances of the theft, we have partnered with Kroll Incorporated, one of the world's leading risk consulting organizations to provide you with the opportunity to enroll in a two-year, free-of-charge, subscription to their credit monitoring and fraud investigation service. The business partner is offering this service to employees, without charge. You will be receiving a packet of information within the next 10 to 14 days, with a unique ID number and instructions on how to activate your membership in this program.

We also recommend and urge you to contact the major credit reporting agencies to place a fraud alert on your credit report, and take advantage of the ID Theft and credit monitoring services provided by Kroll. A fraud alert is your first line of defense in protecting your credit. Details on how to place a fraud alert on your credit file are enclosed. We also encourage you to remain vigilant by reviewing your account statements and monitoring your credit report. Although these are precautionary measures, we feel strongly that it is important for you to take them. Keep in mind that only you can initiate those contacts with your creditors.

In addition, you can obtain information from these sources about the steps the individual can take to avoid identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
Toll Free Number: 1-877-FTC-HELP (1-877-382-4357)
www.ftc.gov

Office of Attorney General
200 St. Paul Place
Baltimore, MD 21202
Toll Free Number in Maryland: 1-888-743-0023
www.oag.state.md.us

If you have any questions or concerns about this information, our Executive Customer Relations team is available to assist you. Please don't hesitate to contact them at 1-800-847-6442 ext 7977. They are available from 8:00 am to 5:00 pm CST Monday – Friday.

Sincerely,



Gary Kusumi
President – GMAC Insurance Personal Lines

Fraud Alert Contact Information

We suggest you contact the fraud departments of any one of the following three major credit-reporting agencies to place a free fraud alert on your credit file. The agency you contact will notify the other two agencies. A fraud alert tells creditors checking the file that recent fraudulent activity has either taken place, or that you are fearful that fraudulent activity may take place in the future. The potential creditor will then know to

contact you before opening new accounts. The fraud alert displays for 90 days and is renewable for subsequent periods.

Experian

PO Box 2002

Allen, TX 75013

To report fraud, call: 1.888.397.3742

www.experian.com

Equifax

PO Box 740241

Atlanta, Ga. 30374

To report fraud, call: 1.800.525.6285

www.equifax.com

TransUnion

PO Box 6790

Fullerton, CA 92834

To report fraud, call: 1.800.680.7289

www.transunion.com

Filing a Credit Fraud Alert with Experian:

There are three credit-monitoring agencies, *Experian, Equifax and TransUnion*. While any one of the three agencies can handle your Credit Fraud Alert report, we found that the **easiest** one to access and file is Experian. Click on "Fraud Alerts" at the bottom of their home page, and then click on the **Initial Security Alert (90 days)** link which will take you to the reporting form. Complete the information, making sure to check the appropriate boxes at the bottom and submit. The process is easy and takes just a few minutes to complete. After completing the required steps, you will receive the following message:

"As you requested, an Initial Security Alert has been added to your credit report. This alert will expire after 90 days from (the date you filed the alert). As an added precaution, we have removed your name from prescreened offer mailing lists for six months.

As a convenience to you, we will notify the other national credit reporting agencies, Equifax and TransUnion, of your request for an Initial Security Alert. You should receive confirmation from them directly.

Click here to view your personal credit report"

What you should know:

Credit Fraud Alerts put potential creditors (financial institutions, retailers, etc.) on notice to carefully check and verify identification **before** extending credit in your name.

Credit Fraud Alerts do not affect your credit score. However, it is important to adequately protect your credit and your credit score by filing a report when incidents like this occur.

Credit Fraud Alerts are available for varying lengths of time, from 90 days in situations like the one we reported, to seven years.

Credit Fraud Alerts are lifted automatically once the time period of the alert has expired.

There is **no cost** for filing a Credit Fraud Alert report.

It is recommended that, along with filing a Credit Fraud Alert report, that you also request a Credit report from the credit-reporting agency you choose. There is no need to request a current credit report from all three agencies as the information is shared among the agencies once it is received.