

**GMAC**  
**Insurance**

## Fax

Date 4/3/08  
Total Pages 22

From Stephen P. Halstead, Assistant General Counsel, GMAC Insurance

To Scott Schafer, Assistant Attorney General  
Company Massachusetts Attorney General's Office  
Fax Number 617 - 727-5765

Regarding GMAC Insurance - Reporting of March 23, 2008 Laptop Theft Incident

Message Dear Mr. Schafer, please see my attached cover letter and other relevant communications to potentially impacted individuals concerning the theft of a laptop from an employee of a GMAC Insurance business partner occurring on March 23, 2008.

**PRIVILEGED AND CONFIDENTIAL**

The information contained in this facsimile is confidential and may also be attorney-client privileged. The information is intended only for the use of the individual or entity to whom it is addressed. If you are not the intended recipient, or the agent or employee responsible to deliver it to the intended recipient, you are hereby notified that any use, dissemination, distribution or copying of this communication is strictly prohibited. If you have received this facsimile in error, please immediately notify us by telephone and return the original message to us at the address below via the U.S. Postal Service. Thank You.



April 3, 2008

Massachusetts Attorney General's Office  
Attn: Scott Schafer, Assistant AG

RE: GMAC Insurance-Reporting of March 23, 2008 Laptop Theft

Dear Mr. Schafer:

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 1 GMACI employee residing in the state of Massachusetts will receive the written notice.

For your records, I have attached the following:

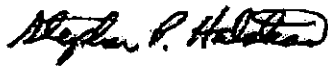
1. First intra-company email to existing employees notifying them of the initial incident;
2. Second intra-company email to existing employees advising them of further developments;
3. Third intra-company email to existing employees advising them of the discovery of the second file containing unencrypted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

①

**Halstead, Steve**

**From:** Office of the CEO  
**Sent:** Wednesday, March 26, 2008 5:01 PM  
**To:** GMAC Ins Employees All  
**Subject:** Important: Employee Security Announcement  
**Importance:** High

**Important Information – Security Breach**

The following communication will be shared with all employees within the next 30 minutes. We would prefer more lead time however, it was important that we share this today. It was decided to provide the information we know at this time and to alert all employees to take appropriate action. As mentioned in the message, more information and detail will follow.

**March 26, 2008**

Yesterday, 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 involved in assisting in the transfer of payroll information associated with our transition to a common GMAC HR system. The incident has been reported to law enforcement authorities and an investigation is underway.

The laptop contained GMACI Personal Lines employee information. It did not contain names, dates of birth or addresses. However, information on the computer includes employees' GMACI-PL user (*Pointsec*) ID sign on and social security number as of the January 11, 2008 payroll date. No other personally identifying information was on the file.

We have been informed by the business partner that the laptop was password protected. For further clarification, this file did not contain any salary or paycheck amounts. Also, there is no connection of the data on the file to any employee by name.

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.

Although we believe the chance of someone using this information to harm you is extremely remote, we do recommend and urge you to contact the major credit reporting agencies to place a fraud alert on your credit report. That is always a good practice.

The business partner will also be offering employees, free of charge, one year of credit monitoring and identity-theft protection. Additional details to follow.

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.

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.

Again, we wanted to inform you of this incident as soon as possible and advise you to place a fraud alert on your

4/3/2008

①

credit report. More information on this and the credit monitoring and identity-theft protection will be shared as soon as it is known.

Sincerely,

Gary Kusumi  
President

**Fraud Alert Contact Information**

We suggest you contact the fraud departments of any one of the three major credit-reporting agencies and let them know you may be a potential victim of identity theft. That agency will notify the other two. Through this process, a "fraud alert" will automatically be placed in each of your three credit reports to notify creditors not to issue new credit in your name without gaining your permission.

**Equifax**

PO Box 740241  
Atlanta, Ga. 30374

To report fraud, call: **1.877.478.7625**  
**www.equifax.com**

**Experian**

PO Box 2002  
Allen, TX 75013

To report fraud, call: **1.888.397.3742**  
**www.experian.com**

**TransUnion**

PO Box 6790  
Fullerton, CA 92834

To report fraud, call: **1.800.680.7289**  
**www.transunion.com**

(2)

**Halstead, Steve**

**From:** Corporate Affairs  
**Sent:** Friday, March 28, 2008 4:15 PM  
**To:** GMAC Ins Employees All  
**Subject:** Reporting A Credit Fraud Alert And Monitoring Credit Activity On Your Account In Two Easy Ways

**Reporting A Credit Fraud Alert And Monitoring Credit Activity On Your Account In Two Easy Ways**

As a follow up to the notification to employees about a stolen laptop containing a file with some employee personal data, we are providing additional information about steps that employees, exercising an abundance of caution, should take:

First, you are encouraged to immediately file a **Credit Fraud Alert** report with one of the three credit reporting agencies. This is your first line of defense in protecting your credit. Details on how to place a Credit Fraud Alert with Experian is provided below.

Next, 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 whose laptop was stolen is offering the service to employees, without charge. More details about this offer are provided below.

**Reporting A Credit Fraud Alert**

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.

**What you should know:**

Credit Fraud Alerts do not affect your credit score. However, failure to adequately protect your credit and your credit score by filing a report when your personal information may have been compromised can result in disastrous consequences.

Once the report is filed with Experian, or any one of the three reporting agencies, the other two agencies are notified.

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

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

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

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.

For answers to more Frequently Asked Questions about credit fraud, click Preventing Fraud.

4/3/2008

②

**Filing a Credit Fraud Alert with Experian**

When you click on **Experian** you will be taken to the **Credit Fraud** page of that agency's site. Take a moment to read the material included on that page.

To file the Credit Fraud Alert report, 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](#)*

**Kroll Credit Monitoring and Fraud Investigation Service Offer**

This service is being offered by the business partner to all employees, free-of-charge. **Kroll Incorporated**, one of the world's largest and most experienced risk assessment and management organizations, will provide the actual credit monitoring and fraud investigation service. Founded in 1972, Kroll provides consultative and support services to individuals, multinational corporations, nonprofit organizations and governmental agencies across the globe.

**Kroll services available to employees:**

- Access to fraud investigators for consultation and answers to questions about ID theft issues
- Recommendations to reduce exposure to ID theft
- Monitoring and monthly reporting of credit activity and any issues identified

**How to apply:**

Kroll, in conjunction with GMACI will be mailing a packet of information to your home within the next 10 to 14 days. This packet will provide you with the necessary information to take advantage of the offer to enroll in the two-year, free-of-charge, subscription to Kroll's credit monitoring and fraud investigation service. The packet will also provide you with a unique ID number and instructions on how to activate your membership.

**If you have questions**

If you have questions, don't hesitate to call the **Customer Relations Team** at 1.800.847.6442, Ext.7977. The team's office hours are from 8 a.m. until 5 p.m. Central Time each business day, Monday through Friday.

③

**Halstead, Steve**

---

**From:** Corporate Affairs  
**Sent:** Tuesday, April 01, 2008 4:06 PM  
**To:** GMAC Ins All  
**Subject:** Important Information – Security Breach Update

April 1, 2008

As a follow up to the notification to employees last week about a stolen laptop containing a file with some employee personal data, we have just learned that a second file on the laptop contained unencrypted employee names and ID numbers. The existence of this file in conjunction with the other file, triggers certain notice requirements under various state "security breach" laws. Employees will be receiving a written "security breach" notice from us in the next few days via the U.S. Postal Service.

Although we continue to believe the chance of someone using this information to harm you is remote, we do recommend and urge you to file a Credit Fraud Alert report with one of the three credit reporting agencies, and to take advantage of the ID Theft and credit monitoring services provided by Kroll.

As previously communicated, the business partner is offering employees, free of charge, two years of credit monitoring and identity-theft protection. Kroll Incorporated, in conjunction with GMACI will be mailing a packet of information to your home within the next 10 to 14 days. This packet will provide you with the necessary information to take advantage of the subscription to Kroll's credit monitoring and fraud investigation service. The packet will also provide you with a unique ID number and instructions on how to activate your membership.

GMAC security policy prohibits personal customer or employee information from being stored on portable devices. 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.

If you have questions, don't hesitate to call the Customer Relations Team at 1.800.847.6442, Ext.7977. The team's office hours are from 8 a.m. until 5 p.m. Central Time each business day, Monday through Friday.

4/3/2008

(4)

**Scripting if leaving a voicemail:** "This is Laura from GMAC Insurance Customer Relations. I am calling to bring a situation to your attention that impacts you as an employee/former employee of GMACI. Please contact Customer Relations as soon as possible to discuss this information. You can reach us at 1-800-847-6442 ext. 7977 between the hours of 8am - 5pm CST. Again that telephone number is 1-800-847-6442 ext. 7977. Thank you."

### Scripting for Outbound Answered Employee Calls

This is Laura from GMAC Insurance Customer Relations. I'm calling to make you aware of a situation that impacts you as a former (leave out the word former if their status code is P = Paid Leave) employee of GMAC Insurance. 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.

The laptop contained two files with unencrypted GMACI employee information as of the January 11, 2008 payroll date. One file contained employees' name and GMACI user (Pointsec) ID sign on. The second file contained employees' GMACI 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.

We will be mailing a letter of notification to you at the mailing address we have on file. Can I verify that address with you to make sure it is accurate? Refer to employee list spreadsheet and verify address. If another address is provided, add it to the "New address" column of the spreadsheet.

GMACI has 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 whose laptop was stolen is offering the 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.

Although we believe the chance of someone using this information to harm you is extremely remote, we do 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. We also encourage you to remain vigilant by reviewing your account statements and monitoring your credit report.

Do you have any questions? Refer to Q&A for answers to any questions asked.

Would you like me to provide you with a web address or phone number you can use to activate a 90-day security alert with Experian? Refer to second page for credit bureau information and instructions on placing the fraud alert.

Callback # for employee if they have any questions - 1-800-847-6442 ext. 7977

Updated: 4/1/08 by Laura Wright

**GMACICON. THESE DOCUMENTS CONTAIN INFORMATION WHICH IS CLASSIFIED AS GMACI CONFIDENTIAL. UNAUTHORIZED REPRODUCTION, DISSEMINATION, MODIFICATION, TRANSMISSION OR DISCLOSURE IS STRICTLY PROHIBITED. COPYRIGHT 2007 GMAC INSURANCE, ALL RIGHTS RESERVED.**



Scripting If leaving a voicemail: "This is Laura from GMAC Insurance Customer Relations. I am calling to bring a situation to your attention that impacts you as an employee/former employee of GMACI. Please contact Customer Relations as soon as possible to discuss this information. You can reach us at 1-800-847-6442 ext. 7977 between the hours of 8am - 5pm CST. Again that telephone number is 1-800-847-6442 ext. 7977. Thank you."

#### Placing a 90 Security alert

#### Filing a Credit Fraud Alert with Experian

Enter the following website, or from the main page at [www.experian.com](http://www.experian.com), click on "fraud alert" at the bottom center of the page.

<https://www.experian.com/consumer/cac/InvalidateSession.do?code=SECURITYALERT>

Take a moment to read the material included on that page.

To file the Credit Fraud Alert report, 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.

Once the report is filed with Experian, or any one of the three reporting agencies, the other two agencies are notified.

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.

Updated: 4/1/08 by Laura Wright

**GMACICOM. THESE DOCUMENTS CONTAIN INFORMATION WHICH IS CLASSIFIED AS GMACI CONFIDENTIAL. UNAUTHORIZED REPRODUCTION, DISSEMINATION, MODIFICATION, TRANSMISSION OR DISCLOSURE IS STRICTLY PROHIBITED. COPYRIGHT 2007 GMAC INSURANCE, ALL RIGHTS RESERVED.**



For answers to more Frequently Asked Questions about credit fraud, click [Preventing Fraud](#).

If the employee would rather utilize a telephone number to place the fraud alert, provide the following information.

**Equifax**

PO Box 740241

Atlanta, Ga. 30374

Fraud Alert - Phone # 800-525-6285

[www.equifax.com](http://www.equifax.com)

**Experian**

PO Box 2002

Allen, TX 75013

To report fraud, call: 1.888.397.3742

[www.experian.com](http://www.experian.com)

**TransUnion**

PO Box 6790

Fullerton, CA 92834

To report fraud, call: 1.800.680.7289

[www.transunion.com](http://www.transunion.com)

Updated: 4/1/08 by Laura Wright

GMACICON. THESE DOCUMENTS CONTAIN INFORMATION WHICH IS CLASSIFIED AS GMACI  
CONFIDENTIAL. UNAUTHORIZED REPRODUCTION, DISSEMINATION, MODIFICATION,  
TRANSMISSION OR DISCLOSURE IS STRICTLY PROHIBITED.  
COPYRIGHT 2007 GMAC INSURANCE, ALL RIGHTS RESERVED.

⑤

CONTENT OF NOTIFICATION BEING MAILED TO MASSACHUSETTS RESIDENTS IMPACTED  
1 RESIDENT POTENTIALLY IMPACTED

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

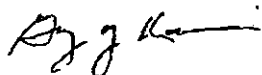
⑤

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.

You have the right under Massachusetts law to obtain a police report, although your opportunity to obtain a report from law enforcement authorities in another jurisdiction may be limited. In addition, you may request that a security freeze be placed on your consumer report by sending a request to a consumer reporting agency. Please review the security freeze information below for more details.

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 and Security Freeze 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.

#### **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.

(5)

**Experian**

PO Box 2002

Allen, TX 75013

To report fraud, call: 1.888.397.3742

[www.experian.com](http://www.experian.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"*

**To place a Security Freeze through Experian:**

The fee for placing a security freeze on a credit report is \$5. If you are a victim of identity theft or spouse of a victim of identity theft and submit a valid investigative or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles (DMV), the fee will be waived. To request a security freeze, log on to [www.experian.com/freeze](http://www.experian.com/freeze) or send all of the following (documentation for both the spouse and the victim must be submitted when requesting the spouse's credit report) to Experian Security Freeze, P.O. Box 9554, Allen, TX 75013: full name, with middle initial and generation, such as JR, SR, II, III, etc.; Social Security number; date of birth (month, day and year); current address and previous addresses for the past two years; and \$5 fee or a valid investigative or incident report or complaint with a law enforcement agency or the DMV. In addition, enclose one copy of a government issued identification card, such as a driver's license, state or military ID card, etc., and one copy of a utility bill, bank or insurance statement, etc. Make sure that each copy is legible (enlarge if necessary), displays your name and current mailing address, and the date of issue (statement dates must be recent).

**Equifax**

PO Box 740241

Atlanta, Ga. 30374

To report fraud, call: 1.800.525.6285

[www.equifax.com](http://www.equifax.com)**To place a Security Freeze through Equifax:**

(5)

For victims of Identity Theft, there is no charge for placing a security freeze through Equifax. For non-victims of Identity Theft, there is a \$5 fee. When you initially request that a state law security freeze be placed on your Equifax credit file you are provided with a security freeze confirmation number which helps facilitate any future actions requested by you regarding the security freeze on your Equifax credit file. If you lose your security freeze confirmation number you must write to us and include the various items listed under Security freeze on Equifax credit file. Please send your request along with proof of your identity to the address below.

NOTE: Consumers in all states can request a security freeze in writing by sending the following information to Equifax (by either certified or regular mail based upon the above grid):

1. Name
2. Address
3. Date of Birth
4. Social Security Number
5. Proof of current address such as a current utility bill
6. Payment of applicable fees to request a security freeze of your credit file.
  - a. Name of the person as it appears on the credit card
  - b. Type of credit card (American Express, Mastercard, VISA, or Discover Card)
  - c. Complete account number
  - d. Expiration data (month and year)
  - e. For American Express - 4 digit Card Identification Number (on front of card above the account number)
  - f. For Mastercard, VISA, or Discover Card - 3 digit Card Identification Number (on back of card at the end of the account number. Please do not send cash through the mail.
7. If you are an identity theft victim and are requesting a security freeze you must also include a copy of a police report, Identity Theft report, or other government law enforcement agency report, such as a DMV report.

Please send your request to the address below.

**Equifax Security Freeze**

P.O. Box 105788  
Atlanta, Georgia 30348  
Phone 800-685-1111

**TransUnion**

PO Box 6790  
Fullerton, CA 92834  
To report fraud, call: 1.800.680.7289  
[www.transunion.com](http://www.transunion.com)

**To place a Security Freeze through TransUnion:**

NOTE: If this is your first time placing a security freeze, there is no fee for requesting a Security Freeze. Once you remove or temporarily lift the Security Freeze, you will be charged up to \$5 to restore the Security Freeze. There is an exception, however, if you are the victim of Identity Theft. You will not

5

be charged this fee if you submit a copy of a police report or a signed copy of a Federal Trade Commission ID Theft victim affidavit.

TransUnion reserves the right to ask for further proof of identity should the information you provide not be complete or if security warrants it. The following can be used as proof of address and Social Security number: copies of current drivers license, bank or credit union statement, Medicaid or Medicare card, paycheck stub, state ID card, W2 form.

Trans Union will accept letters by regular mail, certified mail or overnight mail from the U.S. Postal Service at this address:

**TransUnion**  
Fraud Victim Assistance Department  
P.O. Box 6790  
Fullerton, CA 92834

**Sample Letter:**

Date:

Dear TransUnion:

I would like to place a security freeze on my credit file.

My name is:

Other name(s) used:

My current address is:

My previous address is (if you have other addresses in the previous five years):

My home phone is:

My Social Security number is:

My date of birth is:

My drivers license # is:

Yours Truly,

⑥

## Employee Questions Regarding Privacy Communication

**Q. What date did the theft occur?**

**A. March 23, 2008**

**Q. What information of mine was on the laptop?**

**A. The laptop contained two files with unencrypted employees' information as of the January 11, 2008 payroll date. One file contained employees' GMACI-PL user (Pointsec) ID sign on and social security number; the second file contained employees' GMACI-PL user (Pointsec) ID sign on and name. No other personally identifying information was on the file.**

**Q. Were there any paycheck amounts or salary information on the laptop?**

**A. The file did not contain any salary or paycheck amounts. However, it did contain some deduction amounts that are not identified specifically.**

**Q. It is hard to believe that a payroll file did not contain salary or paycheck amounts.**

**A. The nature of this file did not require that information.**

**Q. Was there any other information on the laptop that if obtained and utilized could be damaging to me?**

**A. Based on information provided by the business partner, we are not aware of any additional information that could be damaging.**

**Q. Was the theft reported to the authorities and have there been any leads in the investigation of the stolen laptop?**

**A. The incident was reported to the Police Department. The case is being investigated and is still open.**

**Q. Where was the laptop stolen?**

**A. The laptop, which was in the possession of an employee of a business partner, was stolen in a home burglary in Ohio.**

**Q. What is the name of the business partner?**

**A. US internetworking, Inc.**

**Q. Why was my information on a laptop belonging to a business partner?**

**A. The information was being used in connection with an assignment involving our payroll system.**

**Q. Was the laptop password protected?**

**A. We have been informed that the laptop was password protected.**

**Q. Was the file containing our information encrypted?**

**A. No. We have been informed that the vendor has been exploring options for encryption, but had not yet deployed a solution. 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.**

**Q. What is the company doing to protect me from possible identity theft?**

**A. In partnership with our business partner, we are offering to all affected employees, free of charge, two years of credit monitoring and identity-theft protection. You should be**

Updated: 4/1/08 by Laura Wright

6

receiving a packet of information in the mail in about 10 business days with an identification number you can use to contact Kroll and activate your service.

- Q. What exactly does the credit monitoring and identity-theft protection do?**  
**A.** This service is being offered by the business partner to all employees, free-of-charge. Kroll Incorporated, one of the world's largest and most experienced risk assessment and management organizations, will provide the actual credit monitoring and fraud investigation service. Founded in 1972, Kroll provides consultative and support services to individuals, multinational corporations, nonprofit organizations and governmental agencies across the globe.

**Kroll services available to employees:**

- Access to fraud investigators for consultation and answers to questions about ID theft issues
- Recommendations to reduce exposure to ID theft
- Monitoring and monthly reporting of credit activity and any issues identified

- Q. Is there anything I can do to prevent identity theft?**  
**A.** You can place a 90 Day Alert on your credit file. In placing a 90 Day Alert on any one of the Credit Bureaus will trigger a 90 Day alert on all three of the Credit Bureaus. It will also trigger a credit report from each of the Credit Bureaus. (Refer to the attachment for contact information for the three Credit Bureaus to place the 90 Day Alert.)

**What you should know:**

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.

Once the report is filed with Experian, or any one of the three reporting agencies, the other two agencies are notified.

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.

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

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.

- Q. What is the true impact of the 90 day alert? For instance if someone makes a payment on an account will the credit bureau be alerted?**  
**A.** **What you should know:**  
 A fraud alert does not result in the credit bureau being alerted when someone makes a payment on your account. A fraud alert tells creditors checking your credit 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

Updated: 4/1/08 by Laura Wright

**GMACICON. THESE DOCUMENTS CONTAIN INFORMATION WHICH IS CLASSIFIED AS GMACI CONFIDENTIAL. UNAUTHORIZED REPRODUCTION, DISSEMINATION, MODIFICATION, TRANSMISSION OR DISCLOSURE IS STRICTLY PROHIBITED.**  
**COPYRIGHT 2007 GMAC INSURANCE, ALL RIGHTS RESERVED.**

6

opening new accounts. The fraud alert displays for 90 days and is renewable for subsequent periods of time.

**Q. Can we be given time during working hours to contact the credit bureaus for the 90 day alert?**

**A. Yes. If you work in one of our call centers, please check with your supervisor or WFM to schedule time off the phones.**

**Q. If I become a victim of identity theft as a result of this incident, what should I do?**

**A. You should immediately contact your creditors and advise them of the incident. If you take advantage of the services offered by Kroll, you should contact them for assistance from a licensed investigator who will work on your behalf to help address and/or correct the identity theft issues you have. They will supply you with a telephone number when you register with them. You may also log onto <http://www.consumer.gov/idtheft/> for more information. Once you have reported the incident, please contact the Customer Relations department at 314-493-7977 to make us aware of the issue.**

**Q. What steps is GMAC insurance taking to ensure this does not happen again?**

**A. As you may be aware through continuing security information posted to our intranet and shared with all employees, privacy is an important issue to us. Please be assured that we are taking this matter seriously and we are working with our business partner and authorities to further investigate this matter. We remain committed to ensuring your privacy and personal information is protected. 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.**

**Q. What steps is our business partner taking to ensure that this does not happen again?**

**A. 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.**

**Q. I am a contractor. Was my information on the file?**

**A. No, Contractor information was not on the file.**

**Q. Are any of our customers impacted?**

**A. No, the file that was on the laptop was limited to GMAC Insurance employees.**

**Q. Was the information in an Excel or Word file, because if so then the computer automatically saves this information to the hard drive?**

**A. Our understanding is that the one file was an Excel spreadsheet saved locally on the laptop hard drive and the second file was in an excel spreadsheet attached in an email.**

**Q. What information determined the criteria for being on the list of employees?**

Updated: 4/1/08 by Laura Wright

**GMACICON. THESE DOCUMENTS CONTAIN INFORMATION WHICH IS CLASSIFIED AS GMACI CONFIDENTIAL. UNAUTHORIZED REPRODUCTION, DISSEMINATION, MODIFICATION, TRANSMISSION OR DISCLOSURE IS STRICTLY PROHIBITED. COPYRIGHT 2007 GMAC INSURANCE, ALL RIGHTS RESERVED.**

6

A. *All GMAC Insurance employees who received a paycheck on 1/11/08 which included deductions for either a 401K, health care or dependant care plan, or health savings plan at that time were on the list.*

**Q. Can information stored on the computer's hard drive be accessed without a password?**

A. *Not to our knowledge, it would be possible for a professional hacker to determine what the password was and then access the system, however the circumstances of the theft indicate that this was not a hacker, but a crime of opportunity.*

**Q. Can a hacker go into the "safe mode" and access the information?**

A. *It would be possible for a professional hacker to determine what the password was and then access the system. However the circumstances of the theft indicate that this was not a hacker, but a crime of opportunity.*

**Q. Was the file administrator privilege password protected?**

A. *Yes the privilege password was protected.*

**Q: Should we change our pointsec passwords?**

A: *There is no need to change your password, as there were no passwords associated with the user ID's in the file. However, you may change your passwords if you wish.*

**Q: Why did you provide my name and address without my permission or consent to a third party?**

A: *Our business partner, with our agreement, has contracted with Kroll to provide credit monitoring because they are one of the world's largest and most experienced risk assessment and management organizations. We take our employee's privacy very seriously and we want to ensure that your identity is completely protected. If you should become a victim of identify theft, although we think this is very unlikely because of the circumstances of the theft, Kroll has an extensive network to assist you.. We provided Kroll with only your name and address, so that they can mail you an informational packet as quickly as possible. You can then decide whether or not to contact them and activate their services.*

**Q. I am not comfortable with you selling my information to another company.**

A. *Your name and address will not be sold; we take your privacy very seriously and your information was not provided to Kroll for their independent use. Our business partner, with our agreement, has entered into contract with Kroll to provide a service to our employees to help protect their identity. You do not have to accept Kroll's services.*

**Q: I know I can go online and get credit monitoring instantaneously, why do I have to wait to receive credit monitoring that will be provided through Kroll?**

A. *Kroll Incorporated will be providing you with packet which explains their services that can meet your needs. We feel that Kroll Inc. is the best company to handle the type of credit monitoring you deserve, with more comprehensive services than the credit monitoring provided by the credit bureaus. While you wait for their packet to arrive in the mail, we suggest you place a Fraud Alert on your credit record.*

**Q. When did the company find out about the additional file?**

Updated: 4/1/08 by Laura Wright

(6)

A. *We were informed by our business partner that there was a second file late in the day on Friday, 3/28/08.*

Q. **What information was contained in the additional file?**

A. *The file contained the unencrypted employee name and GMACI-PL user (Pointsec) ID sign on.*

Q. **Was there any additional information that we were not aware of found in the first file?**

A. *No.*

Q. **How do we know there aren't any more files that contain this type of information?**

A. *Our business partner has conducted a second review of the files and has assured us that there are no additional files and/or information than what we have shared.*

Q. **What is the company doing to ensure there are no other files involved?**

A. *Our business partner has conducted a second review of the files and has assured us that there are no additional files and/or information than what we have shared.*

Q. **How are we holding the business partner accountable?**

A. *We are considering all of our options at this time.*

Q. **In lieu of the situation, has the company's position on the subject of outsourcing changed?**

A. *No, it has not.*

Q. **I work for UWC and never had any issues when I was on their payroll. Why do I have to be on this payroll?**

A. *I do not have any information regarding the payroll system; please contact your HR Representative to discuss this further.*

Q. **I was impacted by this before with GMACI; were there any instances of fraud from that security breach?**

A. *No, there were not.*

Q. **How long is our contract with USI?**

A. *It expires on Dec 31, 2008.*

Q. **Regarding the outbound calls an employee may ask "I don't have time to discuss this over the phone. Can you email me a copy of the internal communications and I'll read them when I have time?"**

A. *We can email you a copy of the formal letter of notification, which will also be mailed to you.*

Q. **Were there other items taken from the business partner employee's home?**

A. *Yes.*

Q. **What else was taken from the business partner employee's home?**

A. *Other computers and a TV were taken.*

Updated: 4/1/08 by Laura Wright

(b)

Updated: 4/1/08 by Laura Wright

**GMAC/CON. THESE DOCUMENTS CONTAIN INFORMATION WHICH IS CLASSIFIED AS GMAC/ CONFIDENTIAL. UNAUTHORIZED REPRODUCTION, DISSEMINATION, MODIFICATION, TRANSMISSION OR DISCLOSURE IS STRICTLY PROHIBITED. COPYRIGHT 2007 GMAC INSURANCE, ALL RIGHTS RESERVED.**