



RECEIVED

April 18, 2008

'08 APR 21 11:35

Stephen H. Levins  
Executive Director, State of Hawaii  
Department of Commerce and Consumer Affairs  
Office of Consumer Protection  
Leiopapa A. Kamehameha Building  
235 South Beretania Street, Suite 801  
Honolulu, Hawaii 96813

STATE OF HAWAII  
CONSUMER PROTECTION

Re: Notification of Security Breach Incident

Dear Mr. Levins:

LendingTree, LLC is writing to notify you of an information security breach involving the personal information of LendingTree's mortgage loan customers.

As you may be aware, LendingTree is an online mortgage lead aggregator; consumers complete loan request forms on LendingTree's website (or over the telephone with LendingTree's Customer Care unit), and LendingTree then matches the consumers with lenders on its network who provide initial mortgage loan offers to the consumers. In addition, LendingTree offers related services under its trade name, "GetSmart." Under the GetSmart program, consumers typically provide less information and are matched with lenders on the network, but the matched lenders do not provide initial mortgage loan offers; instead LendingTree provides contact information to the lender and the consumer.

LendingTree recently discovered that several former employees may have misappropriated passwords that allowed access into LendingTree's files containing customer information. We believe these former employees provided the passwords to three lenders who were not authorized to access LendingTree's customer information. All three lenders were at various times members of the LendingTree network of lenders.

Those three lenders used the passwords to access loan request information to which they were not entitled, and the lenders then solicited the LendingTree (or GetSmart) customers for mortgage loans. The information that the lenders had access to included name, address, email address, telephone number, Social Security number, income and employment information. LendingTree has no indication that the customer information was used for any purpose other than to solicit our customers for mortgage loans. In essence, we believe this situation involves three mortgage companies that wished to market mortgage loans without paying fees to LendingTree. We do not believe this situation involves any fraud on the consumer or identity theft. According to our investigation, we understand that this activity occurred between October 2006 and early 2008.

Stephen H. Levins  
April 18, 2008  
Page 2

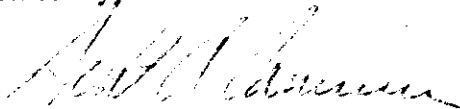
When we discovered the situation in early 2008, we promptly reported the situation to the Federal Bureau of Investigation and we have been cooperating fully with the FBI's investigation. The FBI requested that we not disclose this situation while its investigation was ongoing, because any disclosure could negatively affect the FBI's investigation. The FBI has now indicated that we may disclose this publicly.

LendingTree also conducted extensive internal investigations and took steps to block further access by these lenders and to enhance and strengthen the security of our system and password management. In addition, we brought legal action against the mortgage companies and others involved in this activity.

Based on our internal investigation, on a nationwide basis, LendingTree identified roughly 5,600 LendingTree and GetSmart mortgage customers whose confidential nonpublic information we know was inappropriately accessed by these lenders between December 2007 and early February 2008. These customers are being notified of this situation on Monday, April 21<sup>st</sup>. In addition, we are sending a similar notice to a larger group of mortgage loan customers who submitted LendingTree or GetSmart loan requests during October 2006 through December 2007; with respect to this larger group, we believe the mortgage companies may have in fact accessed the information of only a small percentage of those individuals, but due to system constraints we cannot identify which files were accessed. As a result, we are sending the notification to all of them. The notices include a description of what happened and how customers can obtain free credit reports, place initial fraud alerts and obtain other general information about how to protect their personal information. Again, we have no reason to believe that the information was used in any way other than to solicit the customers for mortgage loans. However, because the information was accessed inappropriately, we concluded it was appropriate to notify affected and potentially affected customers. In total, 8,368 consumers in the State of Hawaii are receiving a notice from LendingTree concerning this incident.

Please feel free to contact me at (704) 943-8248 if you have any questions.

Sincerely,



Scott A. Cammar  
Senior Vice President & General Counsel

Attachments

cc: Mark Merritt, Esq., Robinson Bradshaw & Hinson, P.A.



**April 21, 2008**

**Dear LendingTree Customer:**

We want you to know that recent loan request forms submitted to us by certain customers, including you, were seen by lenders without our consent. These lenders then used the forms to market to those customers the lenders' own mortgage loans. While we don't believe that the forms were used for any other purpose, we want you to know what happened and what we did to correct this situation, as well as what you can do to monitor your credit records.

**What Happened and What We Did**

Recently, LendingTree learned that several former employees may have helped a handful of mortgage lenders gain access to LendingTree's customer information by sharing confidential passwords with the lenders. When we learned of this situation, we quickly contacted the authorities, and LendingTree is helping with their investigation. We promptly made several system security changes. We also brought lawsuits against those involved.

Based on our investigation, we understand that these mortgage lenders used the passwords to access LendingTree's customer loan request forms, normally available only to LendingTree-approved lenders, to market loans to those customers. The loan request forms contained data such as name, address, email address, telephone number, Social Security number, income and employment information. We believe these lenders accessed LendingTree's loan request forms between October 2006 and early 2008.

**What You Can Do**

Again, we don't believe any identity theft or fraudulent financial activity resulted from this situation. However, we suggest you get a free credit report. Look for any accounts you didn't open and/or inquiries from creditors that you didn't initiate. If you see anything you don't understand, contact the credit bureau. If you see anything suspicious, you may want to file a fraud alert with the bureaus. For more information on how to do this, please refer to LendingTree's *Guide to Protecting Your Credit and Identity* (enclosed).

**Where to Get More Information**

We regret any inconvenience and apologize for any unwanted mortgage calls you may have received. For more information about this situation, and for more information on what you can do, please refer to the attached *Questions & Answers Sheet*.

Sincerely

R.L. Harris

## LendingTree's Guide to Protecting Your Credit and Identity

Identity theft occurs when someone uses your personally identifying information – like your name, Social Security number, or credit card number – without your permission to commit fraud or other crimes. All consumers should know about identity theft and what steps they can take to reduce the risk of identity theft or fraud. We suggest that you remain vigilant by reviewing account statements and monitoring your credit reports for the next 24 months.

**Free Credit Reports.** You can get a free copy of your credit report each year at [www.annualcreditreport.com](http://www.annualcreditreport.com) or by calling 1-877-322-8228. When you get your credit report, make sure that all information in the report is current and accurate. If you see any unauthorized transactions or inaccurate information, call the credit bureaus and have the information deleted.

**Fraud Alerts.** If you place a fraud alert in your credit file, potential creditors must either contact you or take additional steps to verify your identity before acting on a credit request. Fraud alerts make it hard for others to steal your identity to get credit. If you think that you've been a victim of identity theft or fraud, contact one of the three major credit bureaus to place a fraud alert on your account. The bureau you contact will forward the fraud alert to the other two bureaus on your behalf, so you don't need to contact all three bureaus yourself. Initial fraud alerts stay on your credit file for 90 days. The bureau will tell you how to extend the fraud alert, which may require you to get a police report or other evidence of identity theft or fraud. Remember that a fraud alert may delay credit approvals.

### Contact the Credit Bureaus

#### Equifax

Office of Fraud Assistance  
P. O. Box 105069  
Atlanta, GA 30348  
(888) 766-0008  
TTY: (866) 478-0030  
[www.equifax.com](http://www.equifax.com)

#### Experian

Credit Fraud Center  
P. O. Box 9532  
Allen, TX 75013  
(888) 397-3742  
TTY: (800) 735-2989  
[www.experian.com](http://www.experian.com)

#### TransUnion

Fraud Victim Assistance Dept.  
P. O. Box 6790  
Fullerton, CA 92834  
(800) 680-7289  
TTY: (877) 533-7803  
[www.tuc.com](http://www.tuc.com)

**For more information:** To learn more about how to protect yourself against identity theft, visit the Federal Trade Commission's identity theft web site at <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/index.html> or call the Federal Trade Commission hotline at 1-877-IDTHEFT (438-4338). You can also call or visit the FTC web site to report any incident of suspected identity theft. You can find resources about identity theft at LendingTree's Smart Borrower Center at <http://www.lendingtree.com/smartborrower/Protecting-Your-Privacy/Protecting-Your-Privacy.aspx>.

IF YOU HAVE ANY QUESTIONS, CONTACT LENDINGTREE AT 866-505-8874

## Questions and Answers

### **Q: What happened at LendingTree?**

Recently, LendingTree learned that several former employees may have taken Company passwords and given them to a handful of lenders. These lenders then used the passwords to access LendingTree customer information files, normally available only to LendingTree-approved lenders, to market loans to LendingTree's customers. The files contained loan request data such as name, address, email address, telephone number, Social Security number, income and employment information.

### **Q: How did you learn about it?**

Our internal security uncovered this situation. We began an internal investigation and reported it to the authorities. We continue to assist the authorities and are telling our customers as soon as it was possible to do so.

### **Q: What kind of customer data was compromised?**

The files contained loan request data such as name, address, email address, telephone number, Social Security number, income and employment information.

### **Q: Was my credit card information compromised?**

No. Credit card information (such as account number or account balance) was not involved.

### **Q: What is being done to prevent this from recurring?**

After LendingTree learned of this situation, we quickly contacted the authorities, and LendingTree is helping with their investigation. We promptly enhanced the security of our system so that this situation couldn't happen again. We also brought lawsuits against the lenders and other persons involved.

### **Q: Is my personal information safe?**

Again, we have no reason to believe any identity theft or fraudulent financial activity resulted from this situation. You still might want to get a free credit report and file a fraud alert with the credit bureaus. When you get your credit report, look for any accounts you didn't open and/or inquiries from creditors that you didn't initiate. If you see anything you don't understand, contact the credit bureau.

### **Q: I didn't apply for a mortgage, but I did apply for a credit card, auto loan, or personal loan. Is my information at risk?**

LendingTree believes that the information accessed was limited to mortgage customer loan requests only, which were then used by the mortgage lenders to solicit those customers for mortgage loans.

IF YOU HAVE ANY QUESTIONS, CONTACT LENDINGTREE AT 866-505-8874

**Q: What should I look for?**

When you get your credit report, look for any accounts you didn't open and/or inquiries from creditors that you didn't initiate. If you see anything you don't understand, contact the credit bureau and discuss your report with them.

**Q: What should I do if I discover suspicious transactions on my credit report?**

If you see anything suspicious, you should contact the credit bureau to report the suspicious transactions and work to have them removed. You may also want to file a fraud alert with the bureaus.

**Q: What is a "fraud alert"?**

If you place a fraud alert in your credit file, potential creditors must either contact you or take additional steps to verify your identity before acting on a credit request. Fraud alerts make it hard for others to steal your identity to get credit. If you think that you've been a victim of identity theft or fraud, contact one of the three major credit bureaus to place a fraud alert on your account. The bureau you contact will forward the fraud alert to the other two bureaus on your behalf, so you don't need to contact all three bureaus yourself. Initial fraud alerts stay on your credit file for 90 days. The bureau will tell you how to extend the fraud alert, which may require you to get a police report or other evidence of identity theft or fraud. Remember that a fraud alert may delay credit approvals.

**Q: Where can I get more information about identity theft?**

You can find resources about identity theft at LendingTree's Smart Borrower Center <http://www.lendingtree.com/smartborrower/Protecting-Your-Privacy/Protecting-Your-Privacy.aspx>, or via the Federal Trade Commission's website at <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/index.html>.

**Q: Who do I call if I have further questions?**

You can call LendingTree at 866-505-8874 to speak with one of our customer service representatives who are available from 9am EST to 9pm EST seven days a week.

**Q: Is there a company contact that I can call to verify that the email or letter I received actually came from LendingTree?**

You can call LendingTree at 866-505-8874 to speak with one of our customer service representatives. Of course, it is always prudent to verify the identity of any person before providing any nonpublic information over the internet, by mail or on the telephone. In particular, never provide personal information in response to emails about security breaches unless you confirm their identity.

IF YOU HAVE ANY QUESTIONS, CONTACT LENDINGTREE AT 866-505-8874

**Q: What mortgage lenders were involved in accessing LendingTree's customer information?**

We brought a lawsuit against Newport Lending Group, Irvine, California; Home Loan Consultants, Inc., Newport Beach, California; and Sage Credit Company, Irvine, California, in connection with this incident.

**Q: Is there any evidence that these lenders used the information for anything other than marketing (e.g., identity theft, etc.)?**

We have no evidence that any identity theft or consumer fraud has resulted from this situation.

**Q: I didn't receive a letter or email. Is my information at risk?**

LendingTree sent emails or letters to the mortgage customers that it believes, based on its investigation to date, might be at risk of having their information accessed and used by these mortgage companies to solicit mortgage loans.

**Q: I applied to LendingTree and heard from several lenders who were not on my official list of LendingTree lenders. Does this mean that my information was accessed, too?**

Whenever you apply for a mortgage loan, you may hear from a variety of lenders. Many mortgage companies purchase what are called "trigger lists" – lists prepared by credit bureaus identifying consumers who have recently had their credit checked – to find out who may be in the market for a mortgage. This is legal although it may result in you hearing from mortgage companies you do not recognize.

If you wish to opt out of the credit bureau's trigger lead program, there are two ways for you to take action. One way is to complete and submit a form online at [www.optoutprescreen.com](http://www.optoutprescreen.com). This method stops trigger leads for five years. The other way is to complete a separate form at the same Web site and then print, sign and mail a letter generated by that form to confirm your opt-out request. This method stops trigger leads permanently.

**Q: What actions can I take to protect myself?**

Again, we have no reason to believe any identity theft or fraudulent financial activity resulted from this situation. In these circumstances, though, it makes sense for you to get a free credit report and check for any irregularities or suspicious transactions, discuss any concerns with the credit bureaus, and consider whether to file a fraud alert. You also should be vigilant for 12 to 24 months in reviewing bank and credit card statements and any future credit reports.

**Q: How can I get a free credit report?**

You can get a free copy of your credit report each year at [www.annualcreditreport.com](http://www.annualcreditreport.com) or by calling 1-877-322-8228.

IF YOU HAVE ANY QUESTIONS, CONTACT LENDINGTREE AT 866-505-8874



April 21, 2008

Dear LendingTree Customer:

We want you to know that some loan request forms our customers sent to LendingTree may have been seen by lenders without our consent. These lenders then used the forms to market their own mortgage loans to our customers. While we don't believe that the forms were used for any other purpose, we want you to know what happened and what we did to correct this situation, as well as what you can do to monitor your credit records.

**What Happened and What We Did**

Recently, LendingTree learned that several former employees may have helped a handful of mortgage lenders gain access to LendingTree's customer information by sharing confidential passwords with the lenders. When we learned of this situation, we quickly contacted the authorities, and LendingTree is helping with their investigation. We promptly made several system security changes. We also brought lawsuits against those involved.

Based on our investigation, we understand that these mortgage lenders used the passwords to access LendingTree's customer loan request forms, normally available only to LendingTree-approved lenders, to market loans to those customers. The loan request forms contained data such as name, address, email address, telephone number, Social Security number, income and employment information. We believe these lenders accessed LendingTree's loan request forms between October 2006 and early 2008.

**What You Can Do**

Again, we don't believe any identity theft or fraudulent financial activity resulted from this situation. However, we suggest you get a free credit report. Look for any accounts you didn't open and/or inquiries from creditors that you didn't initiate. If you see anything you don't understand, contact the credit bureau. If you see anything suspicious, you may want to file a fraud alert with the bureaus. For more information on how to do this, please refer to LendingTree's *Guide to Protecting Your Credit and Identity* (enclosed).

**Where to Get More Information**

We regret any inconvenience and apologize for any unwanted mortgage calls you may have received. For more information about this situation, and for more information on what you can do, please refer to the attached *Questions & Answers Sheet*.

Sincerely

*R. L. Harris*

R.L. Harris

## LendingTree's Guide to Protecting Your Credit and Identity

Identity theft occurs when someone uses your personally identifying information - like your name, Social Security number, or credit card number - without your permission to commit fraud or other crimes. All consumers should know about identity theft and what steps they can take to reduce the risk of identity theft or fraud. We suggest that you remain vigilant by reviewing account statements and monitoring your credit reports for the next 24 months.

**Free Credit Reports.** You can get a free copy of your credit report each year at [www.annualcreditreport.com](http://www.annualcreditreport.com) or by calling 1-877-322-8228. When you get your credit report, make sure that all information in the report is current and accurate. If you see any unauthorized transactions or inaccurate information, call the credit bureaus and have the information deleted.

**Fraud Alerts.** If you place a fraud alert in your credit file, potential creditors must either contact you or take additional steps to verify your identity before acting on a credit request. Fraud alerts make it hard for others to steal your identity to get credit. If you think that you've been a victim of identity theft or fraud, contact one of the three major credit bureaus to place a fraud alert on your account. The bureau you contact will forward the fraud alert to the other two bureaus on your behalf, so you don't need to contact all three bureaus yourself. Initial fraud alerts stay on your credit file for 90 days. The bureau will tell you how to extend the fraud alert, which may require you to get a police report or other evidence of identity theft or fraud. Remember that a fraud alert may delay credit approvals.

### Contact the Credit Bureaus

#### Equifax

Office of Fraud Assistance.  
P. O. Box 105069  
Atlanta, GA 30348  
(888) 766-0008  
TTY: (866) 478-0030  
[www.equifax.com](http://www.equifax.com)

#### Experian

Credit Fraud Center  
P. O. Box 9532  
Allen, TX 75013  
(888) 397-3742  
TTY: (800) 735-2989  
[www.experian.com](http://www.experian.com)

#### TransUnion

Fraud Victim Assistance Dept.  
P. O. Box 6790  
Fullerton, CA 92834  
(800) 680-7289  
TTY: (877) 533-7803  
[www.tuc.com](http://www.tuc.com)

**For more information:** To learn more about how to protect yourself against identity theft, visit the Federal Trade Commission's identity theft web site at <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/index.html> or call the Federal Trade Commission hotline at 1-877-IDTHEFT (438-4338). You can also call or visit the FTC web site to report any incident of suspected identity theft. You can find resources about identity theft at LendingTree's Smart Borrower Center at <http://www.lendingtree.com/smartborrower/Protecting-Your-Privacy/Protecting-Your-Privacy.aspx>.

IF YOU HAVE ANY QUESTIONS, CONTACT LENDINGTREE AT 866-505-8874

## Questions and Answers

### **Q: What happened at LendingTree?**

Recently, LendingTree learned that several former employees may have taken Company passwords and given them to a handful of lenders. These lenders then used the passwords to access LendingTree customer information files, normally available only to LendingTree-approved lenders, to market loans to LendingTree's customers. The files contained loan request data such as name, address, email address, telephone number, Social Security number, income and employment information.

### **Q: How did you learn about it?**

Our internal security uncovered this situation. We began an internal investigation and reported it to the authorities. We continue to assist the authorities and are telling our customers as soon as it was possible to do so.

### **Q: What kind of customer data was compromised?**

The files contained loan request data such as name, address, email address, telephone number, Social Security number, income and employment information.

### **Q: Was my credit card information compromised?**

No. Credit card information (such as account number or account balance) was not involved.

### **Q: What is being done to prevent this from recurring?**

After LendingTree learned of this situation, we quickly contacted the authorities, and LendingTree is helping with their investigation. We promptly enhanced the security of our system so that this situation couldn't happen again. We also brought lawsuits against the lenders and other persons involved.

### **Q: Is my personal information safe?**

Again, we have no reason to believe any identity theft or fraudulent financial activity resulted from this situation. You still might want to get a free credit report and file a fraud alert with the credit bureaus. When you get your credit report, look for any accounts you didn't open and/or inquiries from creditors that you didn't initiate. If you see anything you don't understand, contact the credit bureau.

### **Q: I didn't apply for a mortgage, but I did apply for a credit card, auto loan, or personal loan. Is my information at risk?**

LendingTree believes that the information accessed was limited to mortgage customer loan requests only, which were then used by the mortgage lenders to solicit those customers for mortgage loans.

IF YOU HAVE ANY QUESTIONS, CONTACT LENDINGTREE AT 866-505-8874

**Q: What should I look for?**

When you get your credit report, look for any accounts you didn't open and/or inquiries from creditors that you didn't initiate. If you see anything you don't understand, contact the credit bureau and discuss your report with them.

**Q: What should I do if I discover suspicious transactions on my credit report?**

If you see anything suspicious, you should contact the credit bureau to report the suspicious transactions and work to have them removed. You may also want to file a fraud alert with the bureaus.

**Q: What is a "fraud alert"?**

If you place a fraud alert in your credit file, potential creditors must either contact you or take additional steps to verify your identity before acting on a credit request. Fraud alerts make it hard for others to steal your identity to get credit. If you think that you've been a victim of identity theft or fraud, contact one of the three major credit bureaus to place a fraud alert on your account. The bureau you contact will forward the fraud alert to the other two bureaus on your behalf, so you don't need to contact all three bureaus yourself. Initial fraud alerts stay on your credit file for 90 days. The bureau will tell you how to extend the fraud alert, which may require you to get a police report or other evidence of identity theft or fraud. Remember that a fraud alert may delay credit approvals.

**Q: Where can I get more information about identity theft?**

You can find resources about identity theft at LendingTree's Smart Borrower Center <http://www.lendingtree.com/smartborrower/Protecting-Your-Privacy/Protecting-Your-Privacy.aspx>, or via the Federal Trade Commission's website at <http://www.ftc.gov/bco/edu/microsites/idtheft/consumers/index.html>.

**Q: Who do I call if I have further questions?**

You can call LendingTree at 866-505-8874 to speak with one of our customer service representatives who are available from 9am EST to 9pm EST seven days a week.

**Q: Is there a company contact that I can call to verify that the email or letter I received actually came from LendingTree?**

You can call LendingTree at 866-505-8874 to speak with one of our customer service representatives. Of course, it is always prudent to verify the identity of any person before providing any nonpublic information over the internet, by mail or on the telephone. In particular, never provide personal information in response to emails about security breaches unless you confirm their identity.

IF YOU HAVE ANY QUESTIONS, CONTACT LENDINGTREE AT 866-505-8874

**Q: What mortgage lenders were involved in accessing LendingTree's customer information?**

We brought a lawsuit against Newport Lending Group, Irvine, California; Home Loan Consultants, Inc., Newport Beach, California; and Sage Credit Company, Irvine, California, in connection with this incident.

**Q: Is there any evidence that these lenders used the information for anything other than marketing (e.g., identity theft, etc.)?**

We have no evidence that any identity theft or consumer fraud has resulted from this situation.

**Q: I didn't receive a letter or email. Is my information at risk?**

LendingTree sent emails or letters to the mortgage customers that it believes, based on its investigation to date, might be at risk of having their information accessed and used by these mortgage companies to solicit mortgage loans.

**Q: I applied to LendingTree and heard from several lenders who were not on my official list of LendingTree lenders. Does this mean that my information was accessed, too?**

Whenever you apply for a mortgage loan, you may hear from a variety of lenders. Many mortgage companies purchase what are called "trigger lists" - lists prepared by credit bureaus identifying consumers who have recently had their credit checked -- to find out who may be in the market for a mortgage. This is legal although it may result in you hearing from mortgage companies you do not recognize.

If you wish to opt out of the credit bureau's trigger lead program, there are two ways for you to take action. One way is to complete and submit a form online at [www.optoutprescreen.com](http://www.optoutprescreen.com). This method stops trigger leads for five years. The other way is to complete a separate form at the same Web site and then print, sign and mail a letter generated by that form to confirm your opt-out request. This method stops trigger leads permanently.

**Q: What actions can I take to protect myself?**

Again, we have no reason to believe any identity theft or fraudulent financial activity resulted from this situation. In these circumstances, though, it makes sense for you to get a free credit report and check for any irregularities or suspicious transactions, discuss any concerns with the credit bureau, and consider whether to file a fraud alert. You also should be vigilant for 12 to 24 months in reviewing bank and credit card statements and any future credit reports.

**Q: How can I get a free credit report?**

You can get a free copy of your credit report each year at [www.annualcreditreport.com](http://www.annualcreditreport.com) or by calling 1-877-322-8228.

IF YOU HAVE ANY QUESTIONS, CONTACT LENDINGTREE AT 866-505-8874



U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to  
File No.

400 S. Tryon Street  
Suite 900

January 10, 2008

Lending Tree  
Scott Cammarn  
Information Security Director  
11115 Rushmore Drive  
Charlotte, NC 28277

RE: Request for Non Disclosure

Dear Mr. Scott Cammarn:

The Federal Bureau of Investigation has initiated an investigation into the unauthorized access and possibly criminal breach of Lending Tree's customer database also known as Lender Web Apex. The outstanding cooperation obtained to date from Lending Tree has been instrumental in identifying suspects and various leads.

The FBI respectfully requests that Lending Tree postpone its legal obligation of public disclosure to its valued customers of this potential security breach. Notification at this time may impede the criminal investigation or jeopardize national or homeland security.

Sincerely,

Nathan Gray  
Special Agent in Charge

By: *David E. Johnson*  
David Johnson  
Supervisory Special Agent