

HOMESTEAD FUNDING CORP.

8 Airline Drive, Albany, NY 12205
Office (518) 464-1100 • Fax (518) 464-1141

June 8th, 2015

«Borrower_Name»

«Borrower_Mailing_Addr»

«Borrower_Mailing_City», «Borrower_Mailing_State» «Borrower_Mailing_Zip»

Dear «Borrower_Name»,

We are sending this notification to you as part of Homestead Funding's commitment to customer privacy. We take the protection and proper use of your information very seriously, and it is important to us that you are made fully aware of a potential security incident involving your personal and financial information. On May 21, 2015, Homestead discovered that a cyber attacker carried out a sophisticated attack on our website (<https://homesteadfunding.com>) and we believe the attacker gained unauthorized access to data belonging to some of Homestead's customers over the period of March 27, 2015 through May 10, 2015. Homestead is currently investigating this incident with the assistance of the company that hosts and manages our website.

Immediate Response Taken

As soon as the attack was discovered, we immediately began working with our technology partner responsible for managing our website and secured the site against the attacker. The FBI, Department of Justice, and Baltimore Cybersecurity Task Force were promptly contacted and we have been cooperating fully with their investigation of this incident. Homestead is also undertaking an extensive investigation of the security safeguards concerning our website and customer data so that events like this do not occur again. Homestead has retained an independent information security firm to lead its investigation into the security incident and to assess and strengthen our data security systems.

Information Accessed

The information accessed may have included names, home and work addresses, telephone numbers, dates of birth, driver's license numbers, social security numbers, email addresses, tax and income data, bank and other account numbers, loan data, property information and employment information.

Identity Protection Services

As a precaution, we have arranged to have AllClear ID protect your identity for twelve (12) months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 866-979-2595 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear ID maintains an A+ rating at the Better Business Bureau.

AllClear PRO: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. **You may sign up online at enroll.allclearid.com using the following redemption code: «All_Clear_Numbers»**

Please note: Additional steps may be required by you in order to activate your phone alerts.

What should I do if I have questions?

Call 1-800-724-1329 (extension 378) and ask for Brandy, 9 am to 5 p.m. (EST) Monday through Friday if you have any questions concerning this incident. Contact information for three credit bureaus is listed below.

Fraud Prevention Tips

Homestead wants to make you aware of additional steps that you can take to guard against identity theft and fraud.

We recommend that potentially affected customers remain vigilant for incidents of fraud or identity theft, particularly over the next twelve to twenty-four months, by reviewing account statements and monitoring free credit reports. We also recommend that you change your Homestead password and security questions and answers, and if have any usernames, passwords or security questions and answers for other accounts that are similar to those used in connection with Homestead's website that you change this information too. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate.

We recommend you promptly report suspected incidents of identity theft or suspicious activity by calling your local law enforcement and filing a police report. We suggest that you obtain a copy of the police report as some creditors will want the police report to absolve you of any potential fraudulent debts. To learn more on the subject, you can go to the FTC's website, at www.consumer.gov/idtheft, or call 1-877-ID-THEFT (877-438-4338).

You should be aware of scam email campaigns targeting customers of Homestead. These scams, designed to capture personal information (known as "phishing"), are designed to appear as if they are from Homestead and the emails include a "[click here](#)" link for credit monitoring. These emails

are NOT from Homestead. To protect yourself, we recommend the following if you receive such messages:

- Do NOT reply to the email or reach out to the senders in any way
- Do NOT open any attachments or links that arrive with or that are contained in the email
- Do NOT supply any information on the website that may have opened after you clicked on the email

Homestead will never ask for credit card information or Social Security numbers over the phone in regard to this incident and we recommend that you refrain from providing such information to anyone who contacts you by phone about this security incident. For more guidance on recognizing scam email, please visit the FTC website: <http://www.consumer.ftc.gov/articles/0003-phishing>.

Credit Bureau Information

Equifax P.O. Box 740241 Atlanta, Georgia 30374-0241 1-800-685-1111 www.equifax.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 2000 Chester, PA 19022-2000 1-800-680-7289 www.transunion.com
--	---	--

Fraud Alert and Credit Freeze Information

- *Fraud Alerts*

There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it may also delay your ability to obtain credit. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below. As soon as one bureau processes your fraud alert, it will notify the other two bureaus, which then must also place fraud alerts in your file.

Equifax: 1-800-525-6285, www.equifax.com

Experian: 1-888-397-3742, www.experian.com

TransUnion: 1-800-680-7289, www.transunion.com

- *Credit Freezes (for Non-Massachusetts Residents)*

You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your

credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com

Experian, P.O. Box 9554, Allen, TX 75013, www.experian.com

TransUnion, LLC, P.O. Box 2000, Chester, PA, 19022-2000, www.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

State Specific Information

For Maryland and North Carolina Residents – You can also obtain information from these sources about preventing identity theft:

Maryland

Visit the website:

<http://www.oag.state.md.us/idtheft/index.htm>

Write to this address:

Consumer Protection Division, Identity Theft
Unit
Maryland Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

North Carolina

Visit the website:

<http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims/Security-Breach.aspx>

Write to this address:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001

Call Toll-Free: 1-877-566-7226

We deeply regret that this has happened and any inconvenience or concern caused by this incident.

Sincerely,

Anthony Felitte, COO

AllClear Secure Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required;
- No cost to you – ever. AllClear Secure is paid for by the participating Company.

Services Provided

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services (“Services”) to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period

Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the “Coverage Period”). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements

To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, reside in the United States, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim

If you become a victim of fraud covered by the AllClear Secure services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period.
- Provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company.
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require;
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft;

Coverage under AllClear Secure Does Not Apply to the Following:

Any expense, damage or loss:

- Due to
 - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge
 - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your “Misrepresentation”)
- Incurred by you from an Event that did not occur during your coverage period;
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity;
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur; and
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud;
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of Secure coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

<u>E-mail</u> support@allclearid.com	<u>Mail</u> AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	<u>Phone</u> 1.855.434.8077
--	---	---------------------------------------