

BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400

F 513.929.0303

www.bakerlaw.com

Patrick H. Haggerty
direct dial: 513.929.3412
phaggerty@bakerlaw.com

June 20, 2017

VIA EMAIL (SECURITYBREACH@ATG.WA.GOV) AND OVERNIGHT MAIL

Attorney General Bob Ferguson
Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

Re: Incident Notification

Dear Attorney General Ferguson:

We are writing on behalf of our client, Home Point Financial Corporation (“Home Point”), to notify you of a security incident involving Washington residents.

On March 30, 2017, Home Point learned that an employee had been the target of a phishing email and that an auto-forward rule had been set up in the employee’s email account. Upon learning this, Home Point began an investigation and retained Charles River and Associates (“CRA”) to conduct a forensic investigation. Over the next several weeks, Home Point and CRA reviewed logs and other evidence and determined that a total of 63 Home Point employees fell victim to the phishing campaigns that began in November 2016, which resulted in the employee disclosing their Home Point username and password. In doing so, the employees inadvertently granted access to their Home Point email accounts to unknown individual(s). Home Point has secured the email accounts and reset passwords. Home Point notified Fannie Mae and Freddie Mac of the incident on April 11, 2017. Home Point also notified the FBI and will cooperate in any ensuing investigation.

Home Point is continuing to diligently identify the potentially affected individuals. In early May, CRA determined that the employees’ email accounts contained over 7.2 million documents. CRA was able to extract the documents and conduct a programmatic review using search terms across the data set. That review was completed on May 16, 2017 and narrowed the universe of relevant documents to over 650,000. Since mid-May, a review team of 80

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

Attorney General Bob Ferguson
June 20, 2017
Page 2

individuals, including quality control specialists, has been reviewing the 650,000 documents. The review has taken a significant amount of time and resources because of the volume of documents and the size of the documents (many of the documents are hundreds of pages that need to be manually reviewed). CRA expects to complete the review by the end of this month.

Although the review is ongoing, Home Point has recently identified 815 individuals affected in your state. Some emails and attachments in the affected employees' accounts contained information generally found on or submitted with loan applications including name, address, Social Security number, date of birth, driver's license/passport/state identification number, payment card number, financial account numbers, and for a small number of individuals digital signature, health insurance information, and a password, PIN or account login. Home Point plans to begin notifying affected individuals via U.S. mail on June 27, 2017 in substantially the same form as the letter attached hereto. Home Point will be notifying affected individuals on a rolling basis in order to accelerate the notification process. Notification is being provided as expeditiously as possible. We will provide your Office with an update on the final number of affected Washington residents once the review is complete.

Home Point is offering eligible affected individuals one year of credit monitoring and identity theft resolution services through Experian. Home Point will also provide a call center for potentially affected individuals to call with any questions.

To help prevent a similar incident from happening in the future, Home Point has implemented enhanced security measures and will continue to work to provide employees with awareness and training on how to recognize phishing emails.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



Patrick H. Haggerty
Partner

Enclosure



<Date>

<First Name> <Last Name>

<Address 1>

<Address 2>

<City>, <State>, <Zip>

Dear <First Name> <Last Name>:

Home Point Financial Corporation ("Home Point") is deeply committed to protecting the security and confidentiality of its customers' personal information. Regrettably, we are writing to inform you of an incident involving some of that information.

On March 30, 2017, we learned that an unauthorized individual utilized a phishing scheme and may have gained access to employees' email accounts beginning in November 2016. When we learned of this, we immediately secured the email accounts, reset passwords, and began an investigation. We conducted a thorough review of the employees' email accounts and determined that they contained information that you may have included with your loan application such as your name, address, Social Security number, date of birth, driver's license/passport/state identification number, payment card number, and financial account numbers.

We have no knowledge that your personal information has been misused in any way. However, out of an abundance of caution, we wanted to let you know this happened and assure you we take it very seriously. As a precaution, we are providing you with a complimentary one-year membership for Experian's[®] ProtectMyID[®] Alert. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you and enrolling in this program will not hurt your credit score. **For more information on ProtectMyID Alert, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take, please see the next page of this letter.**

We apologize for any inconvenience or concern this may cause. To help prevent a similar incident from happening in the future, we have implemented improved security measures and will continue to work to provide employees with awareness and training on how to recognize phishing emails. If you have questions regarding this incident, please call toll free to 1-888-721-0151 between 9:00 a.m. and 9:00 p.m. Eastern Time.

Sincerely,

A handwritten signature in black ink that reads "M. Goodman".

Matt Goodman
Chief Administrative Officer
Home Point Financial Corporation

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE That You Enroll By: **[date]** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/alert**
3. PROVIDE Your Activation Code: **[code]**

If you have questions or need an alternative to enrolling online, please call 877-297-7780 and provide engagement #: **[number]**

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
 - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax[®] and TransUnion[®] credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
 - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE[™], which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance***: Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Activate your membership today at www.protectmyid.com/alert or call 877-297-7780 to register with the activation code above.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-297-7780.

Additional Steps You Can Take

Even if you choose not to take advantage of this free credit monitoring, we recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW
Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft