Jeffrey J. Boogay
Office: (267) 930-4784
Fax: (267) 930-4771
Email: jboogay@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

August 29, 2019

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General MacDonald:

We represent Homeside Financial, LLC ("Homeside") located at 5950 Symphony Woods Road, Suite #312, Columbia, MD 21044 and write to notify your office of an incident that may affect the security of some personal information relating to approximately five (5) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Homeside does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On March 29, 2019, Homeside discovered suspicious activity related to certain files from its systems. Homeside immediately launched an investigation to determine the nature and scope of the suspicious file activity. The investigation included working with third-party computer experts. The investigation determined that there was unauthorized access to certain portions of the Homeside system including certain employee email accounts between March 27, 2019 and March 31, 2019. Although the investigation did not conclude that information within the email accounts and system was accessed, the investigation could not rule out this possibility.

In an abundance of caution, Homeside began the process of reviewing the affected email accounts and system to determine if there was any personal information present at the time of the incident. This review required an extensive programmatic and manual review of the affected email accounts and the affected system. Homeside concluded this review on July 3, 2019 and determined that personal information was present in the affected email accounts and system. Since that time, Homeside has been diligently reviewing its records to identify address information for the potentially affected individuals.

The information that could have been subject to unauthorized access includes name, address, and Social Security number.

Notice to New Hampshire Residents

On or about August 29, 2019, Homeside provided written notice of this incident to all affected individuals, which includes approximately five (5) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Homeside moved quickly to investigate and respond to the incident, assess the security of Homeside systems, and notify potentially affected individuals. Homeside is also working to implement additional safeguards and training to its employees. Homeside is providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. Homeside set up a dedicated assistance line for individuals to call should they have additional questions about this incident. Homeside also notified multiple law enforcement authorities of this incident, including the Federal Bureau of Investigation, and is actively cooperating in those investigations.

Additionally, Homeside is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Homeside is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4784.

Very truly yours,

Jeffrey J. Boogay of
MULLEN COUGHLIN LLC

JJB/acl

EXHIBIT A

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

RE: Notice of Data Security Event

Dear <<Name 1>>:

Homeside Financial, LLC ("Homeside") writes to inform you of an incident that may have impacted the security of your personal information. We want to provide you with information about the incident, our response, and steps you may take to better protect against possible misuse of your personal information, should you feel it appropriate to do so.

What Happened? On March 29, 2019, Homeside discovered suspicious activity related to certain files from its systems. Homeside immediately launched an investigation to determine the nature and scope of the suspicious file activity. The investigation included working with third-party computer experts. The investigation determined that there was unauthorized access to certain portions of the Homeside system including certain employee email accounts between March 27, 2019 and March 31, 2019. Although the investigation did not conclude that information within the email accounts and system was accessed, the investigation could not rule out this possibility.

In an abundance of caution, Homeside began the process of reviewing the affected email accounts and system to determine if there was any personal information present at the time of the incident. This review required an extensive programmatic and manual review of the affected email accounts and the affected system. Homeside concluded this review and determined that personal information was present in the affected email accounts and system. Since that time, Homeside has been diligently reviewing its records to identify address information for the potentially affected individuals.

What Information was Involved? A review of email accounts and system involved determined that certain information related to you was present. This information included your name, address, <<Data Elements>>.

What We Are Doing. The confidentiality, privacy, and security of the sensitive information in our care is one of our highest priorities. Upon learning of the incident, we immediately commenced an investigation to confirm its nature and scope and to identify what information may be affected. We also took steps to prevent further unauthorized access to the email accounts and the affected system. While we have measures in place to protect information in our systems, we are reviewing our policies and procedures to improve our existing security. Homeside also notified multiple law enforcement authorities of this incident, including the Federal Bureau of Investigation.

As an added precaution, we are offering you access to twelve (12) months of credit monitoring and identity theft restoration services through TransUnion at no cost to you. Please review the attached "Steps You Can Take to Protect Against Identity Theft and Fraud" for information on these services and instructions on how to enroll. We encourage you to enroll in these services as we are not able to act on your behalf to do so.

What You Can Do. Please review the enclosed "Steps You Can Take to Protect Against Identity Theft and Fraud," which contains information on what you can do to better protect against the possibility of identity theft. You may also enroll in the credit monitoring and identity theft restoration services we are offering, as we are unable to enroll you; you must do so yourself.

For More Information. We understand you may have questions that are not answered in this letter. If you have questions, please contact, 855-958-0572 between 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Friday.

Sincerely,

Homeside Financial, LLC.

Steps You Can Take to Protect Against Identity Theft and Fraud

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for 12 months provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian PO Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion P.O. Box 2000 Chester, PA 19016 1-888-909-8872 www.transunion.com/credit-freeze	Equifax PO Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.