From: Rivera, Kylene (MBS)
Sent: Monday, September 25, 2023 10:54 AM
To: AG CONSUMER [AG] <consumer@ag.iowa.gov>
Cc: Fleitas, Amy M
Subject: Data Breach Reporting- PHH Mortgage Corporation Consumer Data

To whom it may concern-

My name is Kylene Rivera, and I am the Privacy Manager at Phh Mortgage Corporation. I am reporting the following Data Privacy Event on behalf of the Privacy Officer, Assistant General Counsel of Regulatory Affairs, Amy Fleitas.

On June 3, 2023, Pension Benefit Information LLC (PBI), a PHH Mortgage third-party vendor, reported a security event impact with their file transfer software application, MoveIt. MoveIt is widely used across organizations, including the federal government, state governments, universities, healthcare organizations, and enterprise organizations in the United States. MoveIt experienced a zero-day vulnerability, exploited by cyber-security criminals. Although PHH does not utilize MoveIt, PBI uses MoveIt for file-transfers of PHH consumer data to conduct death checks for reverse borrowers.

Immediately upon learning of the MOVEit Transfer vulnerability, PBI completed the recommended patching and remediation steps. They hired forensic investigation firm, Kroll, to assist them in investigating the nature and scope of the vulnerability's impact on their systems. The investigation uncovered that an unknown actor accessed one of PBI's MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded certain data from that system. A review of the impacted data was completed, including a manual validation of the results to identify records associated with PHH Mortgage Corporation. As a result of the entire investigation, PBI reported the event to the federal law enforcement.

On June 16, 2023, PBI disclosed to us that at the time of the event, the name, social security number, date of birth, and address of individuals affiliated with PHH were stored within the impacted MOVEit Transfer server. To date, there have been no reports of identity theft or fraud related to information potentially impacted by this event, and there is no indication any of the obtained information has been released on dark

websites. It was identified that the impacted population included 111,285 individuals, wherein, 501 state residents were included in this population.

On September 5, 2023, PBI confirmed the delivery of consumer notification to all impacted individuals on behalf of PHH Mortgage Corporation, as the data owner.

PHH has worked with PBI to ensure that no file share services nor record retention is performed using Moveit. Additionally, PBI has worked with PBI to redact data points shared back with PHH to eliminate unnecessary additional transport of borrowers' sensitive personal information. PHH confirmed the delivery of consumer notification on behalf of PHH Mortgage Corporation.

I have attached the template used for consumer notification, along with the letter from PBI to PHH, advising of the security event. Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 1-561-629-9778, or by email at amy.fleitas@ocwen.com.

Sincerely,
Kylene Rivera
Privacy Manager
Phh Mortgage Corporation

Pension Benefit Information, LLC
333 South Seventh Street, Suite 2400
Minneapolis, MN 55402

PHH Mortgage Corporation
1661 Worthington Road
Suite 100
West Palm Beach, FL 33409.

June 23, 2023

VIA Email

Pension Benefit Information, LLC ("PBI") writes to inform you of an event that involves certain information related to individuals affiliated with PHH Mortgage Corporation. As you maybe be aware, we utilize the MOVEit Transfer software to securely transfer information on behalf of your organization. Progress Software, the provider of MOVEit Transfer software recently disclosed a zero-day vulnerability affecting its software that had been exploited by cyber criminals. We are providing you with information about the event and our response to it.

Upon learning of the MOVEit Transfer vulnerability, PBI immediately completed the recommended patching and remediation steps. We also promptly launched an investigation into the nature and scope of the vulnerability's impact on our systems with the assistance of third-party cybersecurity specialists. We also reported the event to federal law enforcement. Through the investigation, we learned that an unknown actor accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded certain data from that system. We then undertook a review of the impacted data to determine what information was contained therein and to whom the information related. Additionally, we conducted manual validation of the results of our review to identify records associated with PHH Mortgage Corporation.

Our investigation determined that at the time of the event, the name, social security number, date of birth, and address of individuals affiliated with your organization were stored within the impacted MOVEit Transfer server. Upon request, we will securely send to you a list of those affected individuals. The file names associated with these data elements are listed on Exhibit 1. To date, we have not received any reports of identity theft or fraud related to information potentially impacted by this event.

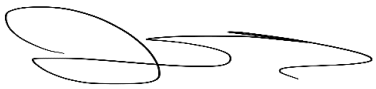
The confidentiality, privacy, and security of information in our possession are among our highest priorities, and we have security measures in place to protect information in our systems. There is no evidence of lateral movement within our environment and the cybersecurity specialists have high confidence that full containment and remediation have been achieved.

You may have certain legal obligations in response to this matter, including providing notice of this event to the individuals affiliated with your organization whose information was contained in the impacted MOVEit Transfer server, and we suggest you share this letter with your organization's legal counsel. You may also have contractual obligations.

We take this event very seriously, and we value our continued partnership. We remain committed to safeguarding your organization's information within our care.

Our understanding is that your preferred form of communication regarding the MOVEit incident is email because of its speed advantage over courier or mail options. If you would like a copy of this letter sent by mail, please send a request to moveitsecurity@pbinfo.com.

Sincerely,



John Bikus
President
Pension Benefit Information, LLC

Exhibit 1

16313_PBI_E_03032023.txt
16313_PBI_E_03062023.txt
16313_PBI_E_03102023.txt
16313_PBI_E_03132023.txt
16313_PBI_E_03172023.txt
16313_PBI_E_03202023.txt
16313_PBI_E_03242023.txt
16313_PBI_E_03272023.txt
16313_PBI_E_03312023.txt
16313_PBI_E_04032023.txt
16313_PBI_E_04072023.txt
16313_PBI_E_04102023.txt
16313_PBI_E_04142023.txt
16313_PBI_E_04172023.txt
16313_PBI_E_04212023.txt
16313_PBI_E_04242023.txt
16313_PBI_E_04282023.txt
16313_PBI_E_05012023.txt
16313_PBI_E_05052023.txt
16313_PBI_E_05082023.txt
16313_PBI_E_05122023.txt
16313_PBI_E_05152023.txt
16313_PBI_E_05192023.txt
16313_PBI_E_05222023.txt
16313_PBI_E_05262023.txt
16313_PBI_E_05292023.txt

10758_01022023.txt
10758_01092023.txt
10758_01162023.txt
10758_01232023.txt
10758_01302023.txt
10758_02062023.txt
10758_02132023.txt
10758_02202023.txt
10758_02272023.txt
10758_03062023.txt
10758_03132023.txt
10758_03202023.txt

10758_03272023.txt
10758_04032023.txt
10758_04102023.txt
10758_04172023.txt
10758_04242023.txt
10758_05012023.txt
10758_05082023.txt
10758_05152023.txt
10758_05222023.txt
10758_05292023.txt
10758_10132022.txt
10758_10172022.txt
10758_10242022.txt
10758_10312022.txt
10758_11072022.txt
10758_11142022.txt
10758_11212022.txt
10758_11282022.txt
10758_12052022.txt
10758_12122022.txt
10758_12192022.txt
10758_12262022.txt
16313_02042022_TEST.txt

<<Return Mail Address>>

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

<<Date>>

<<Notice of Data Breach>>

Dear <<Name 1>> <<Name 2>>:

Pension Benefit Information, LLC ("PBI") provides audit and address research services for insurance companies, pension funds, and other organizations<<, including <<Data Owner>>.[1] PBI is providing notice of a third-party software event that may affect the security of some of your information. Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.

What Information Was Involved? Our investigation determined that the following types of information related to you were present in the server at the time of the event: name and <<Data Elements>>.

What We Are Doing. We take this event and the security of information in our care seriously. Upon learning about this vulnerability, we promptly took steps to patch servers, investigate, assess the security of our systems, and notify potentially affected customers and individuals associated with those customers. In response to this event, we are also reviewing and enhancing our information security policies and procedures.

While we are unaware of any identity theft or fraud as a result of this event, as an additional precaution, PBI is offering you access to <<12/24>> [2]months of complimentary credit monitoring and identity restoration services through Kroll. Details of this offer and instructions on how to activate these services are enclosed with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the enclosed *Steps You Can Take to Protect Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information. You can also enroll in the credit monitoring services that we are offering.

[1] Data Owner to determine whether to include name.
[2] 24 months of credit monitoring to be provided in jurisdictions where more than 12 months are required (Connecticut, Massachusetts, and Washington, DC).

For More Information. If you have additional questions, you may call our toll-free assistance line at <<Kroll Call Center Number>> Monday through Friday from 9:00 am to 11:00 pm Eastern time (excluding U.S. holidays). You may also write to PBI at 333 South Seventh Street, Suite 2400, Minneapolis, MN 55402.

Sincerely,

John Bikus
President
Pension Benefit Information, LLC

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Kroll's Monitoring Services

To help relieve concerns and restore confidence following this event, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<12/24>> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.[3]

Visit **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services.

*You have until **<<Date>>** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional Information

- **Credit Monitoring**. You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.
- **Fraud Consultation**. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.
- **Identity Theft Restoration**. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);

[3] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately [#] Rhode Island residents that may be impacted by this event.