



DLA Piper LLP (US)
1201 North Market Street
Suite 2100
Wilmington, Delaware 19801-1147
www.dlapiper.com
Edward J. McAndrew
Ed.McAndrew@dlapiper.com

March 3, 2022

VIA EMAIL: IDTHEFT&OAG.STATE.MD.US

The Honorable Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Security Incident Notification

Dear Attorney General Frosh:

We are providing notice on behalf of Pulte Mortgage LLC (“Pulte”), pursuant to Md. Code Ann. Comm. Law § 14-3504, about a security incident involving one Maryland resident.

On or about October 27, 2021, the Pulte IT security team discovered an email phishing attempt targeting a single Pulte employee. Pulte immediately launched an investigation into the incident with the assistance of a leading cybersecurity firm. The investigation revealed indicia of unauthorized logins to the email account on October 24 and 25, 2021. Although the employee email account itself appears to have been accessed by an unauthorized individual, Pulte’s investigation revealed no evidence that any email message containing any individual’s personal information was accessed by an unauthorized individual.

Although we do not consider this incident to constitute a data breach under Maryland law, Pulte conducted an analysis of the contents of the relevant employee email account to determine whether the account contained personal information, and to identify and locate any individual whose personal information was contained in the account. On February 24, 2022, Pulte determined that the personal information of one Maryland resident was contained in the email account.

The following types of personal information were contained in the email account for the one Maryland resident: Name and Social Security Number.

Once Pulte became aware of the phishing activity, we immediately launched an investigation with the assistance of leading cybersecurity experts. We secured the relevant email account and we continue to monitor for suspicious activity. We are continuing to enhance our identity, authentication and remote access controls, and to educate our workforce about cybersecurity issues.



VIA EMAIL

March 3, 2022

Page Two

In an abundance of caution, we are notifying potentially affected individual and providing them with access to 24 months of Kroll Identity Monitoring Services, which includes credit monitoring, fraud consultation, and identity theft restoration.

Pulte intends to provide notification to the affected Maryland resident on or about March 4, 2022. A sample of the notification letter is attached.

If you should have any questions or if we can provide further assistance to the Maryland resident affected by this incident, please feel free to contact me at (302) 468-5685 or ed.mcandrew@dlapiper.com.

Respectfully submitted,
DLA Piper LLP (US)

A handwritten signature in blue ink, appearing to be 'EJ McAndrew', written over the printed name.

Edward J. McAndrew

An Attorney for Pulte Mortgage LLC

Enclosure

DATE: [insert]
NAME: [insert]
ADDRESS: [insert]

RE: Notice of Data Security Incident

Dear [Name]:

We write to share important information with you about a data security incident that may have impacted your personal information. The protection of confidential information is among Pulte Mortgage LLC's highest priorities. We sincerely apologize and we take the security of your personal information very seriously.

We want to begin by emphasizing that we have no evidence that your personal information has been accessed without authorization or compromised. In an abundance of caution, we are providing this notice to you so you know what we are doing and the steps you can take to protect your information should you feel it is appropriate to do so.

What Happened? We have conducted an investigation, with the assistance of a leading cybersecurity firm, into email phishing attempt targeting a single Pulte employee. On February 24, 2022, we determined that your personal information was contained in the email account that appears to have been accessed by an unauthorized individual. The dates of potential unauthorized access were October 24 and 25, 2021. Although the employee email account itself appears to have been accessed by an unauthorized individual, our investigation revealed no evidence that any email message containing your personal information was actually accessed by an unauthorized individual.

What Information Was Involved? The types of personal information contained in the email account varied by individual. In general, a limited number of emails contained in the email account may have included one or more of the following types of personal information: Name and Social Security Number.

What We Are Doing. We take this incident, and information security, very seriously. We take numerous actions designed to prevent unauthorized access to our employee email accounts. Upon learning of the phishing activity, we immediately launched an investigation with the assistance of leading cybersecurity experts. We have secured the relevant email account and we continue to monitor for suspicious activity. We are continuing to enhance our identity, authentication and remote access controls, and to educate our workforce about cybersecurity issues.

What You Can Do. As an added precaution, we have arranged to have Kroll, a global leader in risk mitigation and response, provide identity monitoring at no cost to you for two years. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Please 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.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m., Central time, excluding major U.S. holiday. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through Kroll's automated phone system.

For More Information. We sincerely regret any concern this incident may cause you. If you have questions or concerns that are not addressed in this notice letter, please contact our dedicated call center at 1-888-541-3565, where someone will be available to assist you.

Sincerely,

Josh Navin
Customer Liason

Steps You Can Take to Protect Against Identity Theft and Fraud

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.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
800-680-7289
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. Under federal law, you cannot be charged to place, lift or remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax
P.O. Box 105788
Atlanta, GA 30348
800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
888-397-3742

TransUnion
P.O. Box 160
Woodlyn, PA 19094
888-909-8872

Websites:

www.equifax.com/personal/credit-report-services/credit-freeze
www.experian.com/freeze/center.html
www.transunion.com/credit-freeze

To request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail.:

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, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. 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.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement, your state Attorney General, or the Federal Trade Commission. This notice has not been delayed by law enforcement.

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.

District of Columbia Residents: You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
441 4th Street NW
Suite 1100 South
Washington, D.C. 20001

(202) 727-3400
<https://oag.dc.gov/>

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: You may obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft at:

Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
Telephone: 1-888-743-0023.
www.oag.state.md.us/Consumer

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You 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. You can review your 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.

New York Residents: You may obtain information about security breach response and identity theft prevention and protection from the following New York state agencies:

New York Attorney General
Consumer Frauds & Protection Bureau
120 Broadway, 3rd Floor
New York, NY 10271
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, NY 12231
(800) 697-1220
www.dos.ny.gov

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office at:

Office of the Attorney General of North Carolina
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: 1-919-716-6400
www.ncdoj.gov

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

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.

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.