



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Alexandria N. Murphy
Office: (267) 930-1345
Fax: (267) 930-4771
Email: amurphy@mullen.law

40 Burton Hills Boulevard, Suite 200
Nashville, TN 37215

February 9, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Apex Home Loans, Inc. (“Apex”), located at 2400 Research Blvd., Rockville, MD 20950, and are writing to notify your office of an incident that may affect the security of some personal information relating to six hundred and twenty-nine (629) Maryland residents. The response to this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Apex does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about July 30, 2021, Apex discovered suspicious activity related to an employee’s email account. Apex promptly launched an investigation, with the assistance of third-party computer forensic specialists, to confirm the nature and scope of the activity. The investigation determined an unauthorized individual gained access to certain employee email accounts intermittently between May 11, 2021 to July 30, 2021, and may have viewed or obtained emails and/or attachments from within the impacted email accounts.

Apex has been working diligently to perform a comprehensive review of all information contained in the emails and attachments contained within the impacted email accounts. The purpose of this review is to accurately identify any individuals whose personal information may have been present within the impacted emails and therefore accessible to the unauthorized actor. On January 28, 2022, Apex completed this comprehensive review and it was confirmed the following information

relating to Maryland residents was included in the impacted email accounts: name, date of birth, driver's license number, financial account information, payment card information, health insurance information, passport information, and/or Social Security Number. Please note, however, that Apex has no evidence of actual or attempted misuse of any information as a result of the incident.

Notice to Maryland Residents

On or about February 9, 2022, Apex provided written notice of this incident to all potentially affected individuals, which includes six hundred and twenty-nine (629) Maryland 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, Apex moved quickly to investigate and respond to the incident, assess the security of Apex systems, and notify potentially affected individuals. Apex is also working to implement additional safeguards and training to its employees. Apex is providing access to credit monitoring services for twelve (12) months, through Experian to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Apex is providing potentially 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. Apex 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) 930-1345.

Very truly yours,

Alexandria N. Murphy of
MULLEN COUGHLIN LLC

ANM/crm
Enclosure

EXHIBIT A

APEX 
HOME LOANS
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

February 9, 2022

H5300-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



NOTICE OF [Extra1]

Dear Sample A. Sample:

Apex Home Loans writes to inform you of a recent event that may affect the privacy of some of your information. Although we are unaware of any actual or attempted misuse of your information, we are providing you notice of the incident, steps we are taking in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

What Happened? On or about July 30, 2021, Apex Home Loans discovered suspicious activity related to an employee's email account. We promptly launched an investigation to confirm the nature and scope of the activity. The investigation determined an unauthorized individual gained access to certain employee email accounts intermittently between May 11, 2021 to July 30, 2021 and may have viewed or obtained emails and/or attachments from within the impacted email accounts. After conducting a thorough review of the emails and attachments contained within the impacted accounts, which we completed on or about January 28, 2022, we confirmed that some of your information may have been present within the impacted email accounts.

What Information Was Involved? At this time, we are unaware of any actual or attempted misuse of your information as a result of this event. However, we are providing you notice out of an abundance of caution because we confirmed the information present in the potentially impacted files includes your [Extra2].

What We Are Doing. Safeguarding the information entrusted to us is an utmost priority for Apex Home Loans. We responded promptly to this incident and have been working diligently to provide you with accurate and complete notice of the incident as soon as possible. We have taken steps to enhance the security of our systems, including resetting employees' email account passwords. As part of our ongoing commitment to the privacy and security of information in our care, we are reviewing our existing policies and procedures. We are also implementing employee training protocols to mitigate any risk associated with this incident and to better prevent future incidents.

As an added precaution, we are also providing you with 12 months of complimentary access to credit monitoring and identity restoration services through Experian, as well as guidance on how to better protect your information, should you feel it is appropriate to do so. Although we are covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself using the enrollment instructions included in this letter.

0000001



H5300-L01

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. You can find out more about how to better protect against misuse of information in the enclosed *Steps You Can Take To Protect Personal Information*. There, you will also find more information about the credit monitoring services we are offering and how to enroll.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, please call our dedicated assistance line at **(888) 397-0057** (toll-free), Monday through Friday 9:00 am – 11:00 pm EST and Saturday and Sunday 11:00 am – 8:00 pm EST, excluding US holidays. You may also write to us directly at: 2400 Research Blvd., Rockville, MD 20950.

We apologize for any inconvenience this incident may cause you. We remain committed to privacy and security of information in our possession.

Sincerely,

A handwritten signature in black ink that reads "Eric D. Gates". The signature is fluid and cursive, with the first name "Eric" and last name "Gates" clearly legible.

Eric Gates
President

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring Services

To help protect your identity, we are offering a complimentary 12-month membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: **May 31, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: [**https://www.experianidworks.com/credit**](https://www.experianidworks.com/credit)
- Provide your activation code: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(888) 397-0057** by **May 31, 2022**. Be prepared to provide engagement number **B026468** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is not required for enrollment in Experian IdentityWorks.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- Credit Monitoring: Actively monitors Experian file for indicators of fraud.
- Identity Restoration: Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- Experian IdentityWorks ExtendCARETM: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- Up to \$1 Million Identity Theft Insurance²: Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **(888) 397-0057**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.



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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 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 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 your name without your consent. However, you should be aware that using a credit 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 credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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	1-833-395-6938
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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 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 www.oag.state.md.us.

For 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 bureaus 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 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. We encourage you to 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.

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.

