

# **EXHIBIT 1**

By providing this notice, Movement Mortgage LLC (“Movement”) does not waive any rights or defenses regarding the applicability of California law, the applicability of the California data incident notification statute, or personal jurisdiction.

### **Nature of the Data Security Incident**

Earlier this year Movement discovered that several employee email accounts were sending phishing emails. Movement quickly launched an investigation, with the assistance of a third party forensic investigator, to understand the nature and scope of the event and determine whether any sensitive data was at risk. The forensic investigator confirmed that numerous employee email accounts were subject to unauthorized access between October 9, 2017 and March 29, 2018. A review of the affected email accounts was performed using a combination of automated forensic tools and manual document review to determine whether they contained any personal information. On August 1, 2018, Movement determined that the affected email accounts contained personal information of certain loan applicants.

The types of personal information found within the email accounts included different combinations of name and Social Security number, driver’s license number, passport number, taxpayer identification numbers, credit card numbers, and/or bank account information.

### **Notice to California Residents**

On August 31, 2018, Movement will begin mailing written notice of this incident to potentially impacted individuals, including nine thousand, six hundred and five (9,605) California residents. Such notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

### **Other Steps Taken**

Movement is offering affected individuals complimentary access to one year of free credit monitoring and identity restoration services through Experian. Additionally, Movement is providing potentially affected individuals with information on how to protect against identity theft and fraud, including information on how to contact the Federal Trade Commission, the state attorney general, and law enforcement to report any attempted or actual identity theft and fraud. In addition to providing notice of this incident to you, Movement will be providing notice to other state regulators.

Movement has taken several immediate steps to protect against similar incidents in the future. Upon learning of this incident, the email login credentials for all employee email accounts were quickly reset to prevent further unauthorized access. Movement is now specifically monitoring all email accounts for suspicious logins and has implemented multi-factor authentication on all email accounts. Movement is currently reviewing its existing information security procedures and implementing additional training and education for employees to prevent similar future incidents. They have also increased their Information Technology security staff and will continue to implement additional system scanning and monitoring programs going forward.

# **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 Breach**

Dear <<Name 1>>:

Movement Mortgage LLC (“Movement”) is writing to notify you of an incident that may affect the security of some of your personal information. Although we are unaware of any actual or attempted misuse of your information, we are providing you with information regarding the incident, steps we have taken since discovering the incident, and what you can do to protect against identity theft and fraud should you feel it is appropriate to do so.

**What Happened?** Earlier this year Movement discovered several of our employee email accounts were sending phishing emails. Movement quickly launched an investigation, with the assistance of a third party forensic investigator, to understand the nature and scope of the event, and whether any sensitive data was at risk. The forensic investigator confirmed that numerous employee email accounts were subject to unauthorized access between October 9, 2017 and March 29, 2018. We then reviewed the affected email accounts to determine whether they contained any personal information. On August 1, 2018, Movement Mortgage determined that the affected email accounts contained personal information of certain loan applicants, including you.

<<Data Element Paragraph>>

**What Are We Doing?** Information privacy and security are among our highest priorities. Movement has strict security measures to protect the information in our possession. Upon learning of this incident, we quickly reset the email login credentials for all employee email accounts to prevent further unauthorized access. We are currently implementing additional training and education for employees to prevent similar future incidents. We are also specifically monitoring all email accounts for suspicious log-ins and implemented multi-factor authentication on all email accounts. We have also increased our Information Technology security staff and will continue to implement additional system scanning and monitoring programs going forward.

**What Can You Do?** Although we are not aware of any actual or attempted misuse of your information, we arranged to have Experian protect your identity for 1 year at no cost to you as an added precaution. Please review the instructions contained in the attached “Steps You Can Take to Protect Your Information” to enroll in and receive these services. Movement will cover the cost of this service; however, you will need to enroll yourself in the credit monitoring service.

**For More Information:** We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 866-287-3696 (toll free), Monday through Friday, 9:00 a.m. to 9:00 p.m., ET.

We sincerely regret any inconvenience this incident may cause you. Movement remains committed to safeguarding information in our care and we will continue to take steps to ensure the security of our systems.

Sincerely,

A handwritten signature in black ink, appearing to read "Joseph Dinolfo". The signature is stylized with a large, sweeping initial "J" and "D".

Joseph Dinolfo  
Director of Compliance, Movement Mortgage

## Steps You Can Take to Protect Your Information

### **Enroll in Credit Monitoring:**

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks<sup>SM</sup> Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

### **Activate IdentityWorks Credit 3B Now in Three Easy Steps**

1. **ENROLL** by: <<Enrollment Deadline>> (Your code will not work after this date.)
2. **VISIT** the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. **PROVIDE** the **Activation Code:** <<Enrollment Code>>

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 877-288-8057. Be prepared to provide engagement number <<Engagement Number>> as proof of eligibility for the identity restoration services by Experian.

### **ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:**

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE<sup>TM</sup>:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance<sup>\*\*</sup>:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-288-8057 to register with the activation code above.**

**What you can do to protect your information:** There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration) for this information. If you have any questions about IdentityWorks, 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 877-288-8057.

### **Monitor Your Accounts.**

To further protect against possible identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity.

**Credit Reports.** 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](http://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.

**Fraud Alerts.** 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 19016  
800-680-7289  
www.transunion.com

**Security Freeze.** 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. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, depending on your residence, a credit bureau may charge you a fee to place, temporarily lift, or permanently 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 Security Freeze  
P.O. Box 105788  
Atlanta, GA 30348  
1-800-685-1111  
<https://www.freeze.equifax.com>

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

TransUnion  
P.O. Box 2000  
Chester, PA 19016  
1-888-909-8872  
[www.transunion.com/securityfreeze](http://www.transunion.com/securityfreeze)

**Additional Information.** You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state’s Attorney General. **For Maryland residents,** the Attorney General can be contacted by mail at 200 St. Paul Place, Baltimore, MD, 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at [www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov). **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 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 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](http://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 North Carolina Residents:** The North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400, and online at [www.ncdoj.gov](http://www.ncdoj.gov). **The Federal Trade Commission** can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as a result of a law enforcement investigation.