

# ALSTON & BIRD

The Atlantic Building  
950 F Street, NW  
Washington, DC 20004-1404  
202-239-3300 | Fax: 202-239-3333

RECEIVED

SEP 01 2021

CONSUMER PROTECTION

Kimberly Peretti

Direct Dial: 202-239-3720

Email: Kimberly.Peretti@alston.com

August 31, 2021

**CONFIDENTIAL  
VIA OVERNIGHT DELIVERY**

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

Re: Notice of Data Security Incident

To the Office of the New Hampshire Attorney General:

We are writing on behalf of our client, MFA Financial, Inc. ("MFA"), to notify you of a data security incident that may have affected the personal information of residents in your state. A copy of the notification being sent to 22 New Hampshire residents by first class mail on September 1, 2021 is attached to this letter.

On March 10, 2021, MFA suffered a cybersecurity incident in its legacy environment. Upon discovery, MFA took immediate steps to contain the threat and engaged a third-party forensics firm to investigate the incident and assist with remediation efforts. MFA also notified federal law enforcement authorities of the incident.

MFA's investigation has found that, between February 12, 2021 and March 10, 2021, an unauthorized party was able to access and remove data from a file server in MFA's legacy environment, which contained personal information pertaining to MFA employees and certain individuals that may have been listed as dependents and/or beneficiaries in employee insurance documentation. The legacy file server also contained limited personal information of the owners of loans and mortgages in which MFA and its subsidiaries invest.

As a result of MFA's ongoing investigation, on August 2, 2021, MFA was able to determine that personal information of certain residents in your state may have been involved. The personal information may have included: name, address, date of birth, and Social Security number.

August 31, 2021

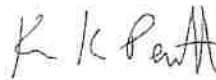
Page 2

MFA takes the security of personal information very seriously. As soon as MFA discovered the incident, MFA promptly launched a forensic investigation, contacted law enforcement, and took steps to remediate the incident. In response to this incident, MFA has enhanced its security and monitoring and taken other measures to minimize the risk of a similar incident in the future.

MFA has arranged to offer credit monitoring, identity theft protection, and Dark Web monitoring services for a period of two years to the impacted residents whose personal information may have been involved.

If you have any questions regarding this event or if you desire further information or assistance, please email me at [Kimberly.Peretti@alston.com](mailto:Kimberly.Peretti@alston.com) or call my direct line at (202) 239-3720.

Sincerely,

A handwritten signature in black ink, appearing to read "K Peretti". The signature is written in a cursive style with a large initial "K" and a stylized "Peretti".

Kimberly Peretti

Enclosures



C/O IDX  
P.O. Box 1907  
Suwanee, GA 30024

<<First Name>> <<Last Name>>  
<<Address1>> <<Address2>>  
<<City>>, <<State>> <<Zip>>

September 1, 2021

#### **Notice of Data Security Incident**

To <<First Name>> <<Last Name>>,

We are writing to inform you about a data security incident that may have affected your personal information.

#### **Who is MFA?**

MFA Financial, Inc. ("MFA" or "we") is a real estate investment trust. MFA, through its subsidiaries (including its various MFRA Trusts), is primarily engaged in the business of investing in residential mortgage assets, including residential whole loans and residential mortgage-backed securities. In connection with our and our MFRA Trust subsidiaries' investment in residential whole loans, we may have information pertaining to the borrowers on certain mortgage loans.

#### **What happened?**

On March 10, 2021, MFA suffered a cybersecurity incident in its legacy environment. Upon discovery, we took immediate steps to contain the threat and engaged a third-party forensics firm to investigate the incident and assist with remediation efforts. We also notified federal law enforcement authorities of the incident.

Our investigation has found that, between February 12, 2021 and March 10, 2021, the unauthorized party was able to access and remove data from a file server in our legacy environment, which contained limited personal information of the owners of loans and mortgages in which we and our subsidiaries invest.

#### **What information may have been involved?**

As a result of our ongoing investigation, on August 2, 2021, we were able to determine that your personal information may have been involved. The personal information may have included: name, address, date of birth and Social Security number.

#### **What we are doing.**

MFA takes the security of personal information very seriously. As soon as we discovered the incident, we promptly launched a forensic investigation, contacted law enforcement, and took steps to remediate the incident. In response to this incident, we have enhanced our security and monitoring and taken other measures to minimize the risk of a similar incident in the future.

We have arranged to offer you credit monitoring, identity theft protection, and Dark Web monitoring services for a period of two years, at no cost to you, through IDX. You have until December 1, 2021 to activate these services, and instructions on how to activate these services are included in the attached Reference Guide.

**What you can do.**

In addition to signing up for your complimentary credit monitoring, the enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your personal information. We encourage you to carefully review credit reports and account statements to ensure that all of your account activity is valid. Any questionable charges should be promptly reported to the company with which the account is maintained.

**For more information**

If you have any questions about this matter or would like additional information, please refer to the enclosed Reference Guide, visit <https://app.idx.us/account-creation/protect>, or call toll-free 833-664-1799. The call center is open from 9:00 AM to 9:00 PM Eastern time, Monday through Friday, except holidays.

We regret that this incident occurred and apologize for any inconvenience this incident may have caused you.

Sincerely,

Harold E. Schwartz  
Senior Vice President & Secretary

## **Reference Guide**

### **Review Your Account Statements**

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained.

### **Order Your Free Credit Report**

To order your free annual credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com), call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at [www.ftc.gov](http://www.ftc.gov) and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

### **How to Enroll in IDX Credit Monitoring Protection**

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service for two years provided by IDX.

To enroll in this service, please call 833-664-1799 or visit <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using Enrollment Code: [ENROLLMENT CODE]

The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

### **Contact the U.S. Federal Trade Commission**

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW

Washington, DC 20580  
1-877-IDTHEFT (438-4338)  
[www.ftc.gov/idtheft/](http://www.ftc.gov/idtheft/)

### **Place a Fraud Alert on Your Credit File**

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	888-766-0008	<a href="http://www.equifax.com">www.equifax.com</a>
Experian	P.O. Box 9554 Allen, Texas 75013	888-397-3742	<a href="http://www.experian.com">www.experian.com</a>
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	<a href="http://www.transunion.com">www.transunion.com</a>

### **Security Freezes**

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	800-685-1111	<a href="http://www.equifax.com">www.equifax.com</a>
Experian Security Freeze	P.O. Box 9554	888-397-3742	<a href="http://www.experian.com">www.experian.com</a>

Allen, TX 75013

TransUnion

P.O. Box 160  
Woodlyn, PA 19094

888-909-8872

www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

#### **For Residents of the District of Columbia**

You may contact the D.C. Attorney General's Office to obtain information about steps to take to avoid identity theft:

D.C. Attorney General's Office, Office of Consumer Protection, 400 6<sup>th</sup> Street, NW, Washington DC 20001, 1-202-442-9828, [www.oag.dc.gov](http://www.oag.dc.gov).

#### **For Residents of Iowa**

You may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft. The Iowa Attorney General's Office can be reached at:

Iowa Attorney General's Office, Director of Consumer Protection Division, 1305 E. Walnut Street, Des Moines, IA 50319, 1-515-281-5926, [www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov).

#### **For Residents of Maryland**

You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, <http://www.marylandattorneygeneral.gov/>.

#### **For Residents of New Mexico**

New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal.

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

- (1) the unique personal identification number, password or similar device provided by the consumer reporting agency;
- (2) proper identification to verify your identity;

(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of pre-screening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

**For Residents of New York**

You may also obtain information about security breach response and identity theft prevention and protection from the New York Attorney General's Office:

Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, [www.ag.ny.gov](http://www.ag.ny.gov).

**For Residents of North Carolina**

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6000, [www.ncdoj.gov](http://www.ncdoj.gov).

**For Residents of Oregon**

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for the Oregon Department of Justice is as follows:

Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301, 1-877-877-9392, [www.doj.state.or.us](http://www.doj.state.or.us)

2021 SEP - 1 AM 10: 22

STATE OF NH  
DEPT OF JUSTICE