THOMPSON COBURN LLP

55 East Monroe Street
37th Floor
Chicago, IL 60603

312 346 7500 main
312 580 2201 fax
thompsoncoburn.com

Melissa K. Ventrone
312 580 2219 direct
mventrone@thompsoncoburn.com

March 9, 2018

VIA ELECTRONIC MAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Dear Attorney General Frosh:

We represent Academy Mortgage Corporation ("Academy") with respect to a recent data security incident involving the potential exposure of personally identifiable information described in more detail below. Academy is a mortgage company with locations across the United States.

1. Nature of security incident.

On January 24, 2018, Academy learned that direct deposit bank account information for a limited number of employees was changed within Workday, Academy's payroll application. The Workday product is not resident within Academy's systems, but instead is in a hosted environment controlled by a third-party vendor.

As soon as Academy learned of the incident, it immediately began an internal investigation, and requested that Workday provide detailed access information for the suspect accounts. Academy determined that an unauthorized individual compromised a small number of employees' log-in credentials through a phishing scam. The credentials were then used to access those specific employees' Workday accounts to replace direct deposit information with unauthorized pre-paid payment card numbers. Academy was able to stop the transfer of funds, and prevented any funds from being sent to unauthorized accounts.

Only direct deposit account information appeared to have been accessed by the unauthorized individual. However, Workday contains the Social Security numbers of employees, and may contain the names and Social Security numbers of any beneficiaries or dependents of the employee. Although there is no evidence that this information was accessed or acquired by the unauthorized person, Academy provided notification to all impacted employees' beneficiaries and dependents out of an abundance of caution.

2. Number of Maryland residents affected.

Seven (7) Maryland residents were impacted by this incident. A notification letter was sent to the affected individuals on March 9, 2018 via regular mail (a copy of the form notification letter is enclosed).

3. Steps taken or plan to take relating to the incident.

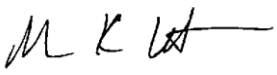
Academy is taking steps to help prevent this type of incident from occurring in the future, including requiring administrative approval to change direct deposit account information within Workday, and providing training materials to employees about how to avoid falling victim to phishing scams. Academy has reported this incident to law enforcement and is cooperating with their investigation. Additionally, affected individuals were offered credit monitoring and identity restoration services free of charge for one year through AllClear ID.

4. Contact information.

Academy remains dedicated to protecting the confidential information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at MVentrone@ThompsonCoburn.com or (312) 580-2219.

Very truly yours,

Thompson Coburn LLP



Melissa K. Ventrone

Enclosure

ACADEMY
MORTGAGE CORPORATION®

Diane Cask
12927 S Boulter St.
Draper, UT 84020

3/9/2018

Notice of Security Incident

Dear Diane Cask:

We wanted to provide you with additional information regarding the recent security incident involving our payroll application, Workday. We value and respect the privacy of your information, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

1. What happened and what information was involved:

On January 24, 2018, Academy Mortgage Corporation ("Academy") learned that direct deposit bank account information for a limited number of employees was changed within Workday. We immediately began an internal investigation, and determined that an unauthorized individual was able to access Workday after compromising a small number of employees' log-in credentials through a phishing scam. The unauthorized access appears to have started on January 18, and ended January 24, 2018 when we reset all employee passwords. Although your direct deposit information was changed, we were able to stop any funds from being transferred to a fraudulent account and your pay was not impacted. We have no evidence that anything other than your bank account information was viewed, however Workday also contains your Social Security number, date of birth, and other sensitive information.

2. What we are doing and what you can do:

Because Workday contains your sensitive information, out of an abundance of caution we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-865-6899 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-865-6899 using the following redemption code: 1485460578.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

We are taking steps to help prevent this type of incident from occurring in the future, including requiring administrative approval to change direct deposit account information within Workday, and providing training materials to employees about how to avoid falling victim to phishing scams. We have reported this incident to law enforcement and are cooperating with their investigation.

4. For more information:

If you have any questions or concerns, please call 1-855-865-6899 Monday through Saturday, 8 am to 8 pm Central Time. Your trust is a top priority for Academy, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Christina L. Baker

Christina Baker
Executive Vice President, Human Resources
Academy Mortgage Corporation

U.S. State Notification Requirements

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon,* and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 6790
Fullerton, CA 92834
1-800-916-8800
www.transunion.com

You may also obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*:
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*:
State laws advise you to report any suspected identity theft to law enforcement, the Oregon Attorney general, as well as the Federal Trade Commission.

For residents of *Maryland, North Carolina,* and *Rhode Island*:
You can obtain information from your state's Attorneys General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft, contact information for whom is provided below:

Maryland Attorney General
Consumer Protection Div.
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

North Carolina Attorney General
Consumer Protection Div.
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Rhode Island Attorney General
Consumer Protection Div.
150 South Main Street
Providence, RI 02903
(401) 274-4400
www.riag.ri.gov

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.identityTheft.gov

For residents of *Massachusetts*:
It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:
Fraud Alerts: You can place fraud alerts with the three credit bureaus at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three credit bureaus is below.
Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.
Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to send a request to each consumer reporting agency by certified mail, overnight mail, or regular stamped mail. 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. The consumer reporting agency may charge a fee of up to $5.00 to place a freeze or lift or remove a freeze, but is free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://www.experian.com/freeze

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
www.transunion.com

More information can also be obtained by contacting the Federal Trade Commission listed above.

AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements
To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail	Mail	Phone
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077