

**LEWIS
BRISBOIS
BISGAARD
& SMITH LLP**
ATTORNEYS AT LAW

1055 Westlakes Drive, Suite 300
Berwyn, Pennsylvania 19312
Telephone: 215.977.4100
Fax: 215.977.4101
www.lewisbrisbois.com

SIAN M. SCHAFLE
DIRECT DIAL: 215.977.4067
SIAN.SCHAFLE@LEWISBRISBOIS.COM

April 25, 2014

VIA U.S. MAIL

Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: JCM Partners — Notice of Data Security Event

Dear Sir or Madam:

We represent JCM Partners, LLC (“JCM”), 2151 Salvio Street, Suite 325, Concord, CA, 94520 and are writing to notify you of a data event that may have compromised the security of personal information of four (4) New Hampshire residents. JCM’s investigation into this event is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, JCM does not waive any rights or defenses under New Hampshire law.

Nature of the Data Security Event

On March 6, 2014, JCM learned that unauthorized individuals accessed a JCM database containing personal information of JCM housing applicants and posted this information on an unauthorized website. JCM immediately removed the file from the unauthorized website. JCM launched an internal investigation. JCM retained a nationally recognized independent, third-party security expert to assist with this investigation. From this investigation, JCM believes that unauthorized individual(s) committed a sophisticated, criminal intrusion of a JCM database containing information inputted into JCM’s website by its applicants. The unauthorized individual(s) posted some of the information from the database on an unauthorized website.

JCM secured its affected database and removed personal information relating to its housing applicants from the database. JCM and its security expert reviewed all available data in an effort to determine what information may have been accessed. Although these investigations are ongoing, it

is possible that unauthorized individual(s) may have accessed the names, addresses, Social Security numbers, driver's license numbers, and email addresses of four (4) New Hampshire residents.

Notice to New Hampshire Residents

JCM sent written notice of this incident to the four (4) residents on April 24, 2014, in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

In addition to providing written notice of this incident to the affected individuals as described above, each affected individual is being offered access to one (1) free year of identity monitoring services and identity restoration services. JCM is also providing each individual with information regarding how to protect against identity theft and fraud. JCM is providing written notice of this incident to other state regulators and to the national consumer reporting agencies.

JCM is also working with a security expert to take steps to further protect the security of personal information at JCM.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 215-977-4067.

Very truly yours,



Sian M. Schafle for
LEWIS BRISBOIS BISGAARD & SMITH LLP

SMS:lpt
cc: JCM Partners

Exhibit A



Processing Center · P.O. Box 3825 · Suwanee, GA 30024

April 24, 2014



John Sample
123 Main Street
Anytown, US 12345-6789



Dear John Sample,

JCM Partners (“JCM”) is writing to inform you of an incident that may have involved some of your personal information. This incident may have resulted in unauthorized access to personal information including your name, Social Security number, driver’s license number, email address and mailing address. We are providing this notice to you so that you may monitor your financial statements and take steps to protect your information.

On March 6, 2014, JCM learned that a file containing personal information of housing applicants was taken from a JCM database and posted on an unauthorized website. We immediately removed the file from the unauthorized website. We launched an internal investigation to determine what information may have been accessed by unauthorized individual(s). We retained an independent, third-party security expert to assist with this investigation. Working with this security expert, we also took steps to better protect the security of personal information at JCM. The investigation is ongoing.

JCM has not received any reports of fraud or identity-related crimes relating to this incident. Nevertheless, as an added precaution, 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 SECURE: The team at AllClear ID is ready and standing by if you need help protecting your identity. You are automatically eligible to use this service – there is no action required on your part. If a problem arises, simply call (877) 979-2595 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear maintains an A+ rating at the Better Business Bureau.

AllClear PRO: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use the PRO 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 (877) 979-2595 using the following redemption code: 9999999999.

Please note: Additional steps may be required by you in order to activate your phone alerts.



0102000001

We also encourage you remain vigilant, to review your account statements regularly, 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 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. Information regarding security freezes is also available from these agencies.

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

You can further educate yourself regarding identity theft, security freezes, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-ID-THEFT (877-438-4338); TTY: 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. Instances of known or suspected identity theft should also be reported to law enforcement. This notice was not delayed because of law enforcement.

JCM apologizes for any inconvenience or concern that this caused you. The safety and security of your personal information remains a top priority of JCM. We have established a confidential privacy line to assist you with any questions regarding the incident, this letter or AllClear's identity monitoring services. This confidential privacy line can be reached at (877) 979-2595, Monday through Saturday, 8:00 a.m. to 8:00 p.m. CST.

Sincerely,



Brian Rein
Chief Operation Officer
JCM Partners

Terms of Use for AllClear Secure

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:

- Automatic 12 months of coverage;
- No cost to you – ever. AllClear Secure 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 Secure 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

You are automatically protected for 12 months from the date the breach incident occurred, as communicated in the breach notification letter you received from Company (the “Coverage Period”). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements

To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen eighteen (18) years of age or older, reside in the United States, 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 Secure services, you must:

- Notify AllClear ID by calling 1.855.434.8075 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Secure 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;
- 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 Secure 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
 - 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;
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure 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 Secure 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; and
- You are expected to protect your personal information in a reasonable way at all times. Accordingly, you will not recklessly disclose or publish your Social Security number or any other personal information to those who would



reasonably be expected to improperly use or disclose that Personal Information, such as, by way of example, in response to "phishing" scams, unsolicited emails, or pop-up messages seeking disclosure of personal information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

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