



150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

April 27, 2023

Michael J. Waters
Shareholder
312.463.6212
312.873.2918 Fax
mwaters@polsinelli.com

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notification of a Data Security Incident

Dear Madam/Sir:

We represent VCC, LLC (“VCC”), 1 Information Way Suite 300, Little Rock, AR 72202, in connection with a recent incident that may have involved the personal information of one (1) Maryland resident. VCC is reporting the incident pursuant to MD. CODE ANN., COM. LAW § 14-3504(H). This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to this submission. While VCC is notifying you of this Incident, VCC does not waive any rights or defenses relating to the incident or this notice, or the applicability of Maryland law on personal jurisdiction.

NATURE OF THE SECURITY INCIDENT

On February 07, 2023, VCC discovered suspicious activity on its computer network. Upon discovering the incident, VCC promptly initiated an internal investigation to prevent further unauthorized access, began restoring its systems from viable backups, notified law enforcement, and engaged a forensic security firm to further investigate and secure its computer systems. The forensic investigation determined that an unknown, unauthorized third party gained access to its computer systems on February 3, 2023, and determined that certain personal information may have been accessed and/or acquired as a result of the incident. VCC conducted a comprehensive review of the involved files to determine if it contained any personal information. On March 15, 2023, it was determined that the files contained some personal information, which included the name and Social Security number of one (1) Maryland resident. At this point, VCC is not aware of any fraud or identity theft to any individual as a result of this incident.

polsinelli.com

Atlanta Boston Chicago Dallas Denver Houston Kansas City Los Angeles Miami Nashville New York
Phoenix St. Louis San Francisco Seattle Silicon Valley Washington, D.C. Wilmington

Polsinelli PC, Polsinelli LLP in California
89426924.1

April 27, 2023

Page 2

NUMBER OF MARYLAND RESIDENTS AFFECTED

On April 27, 2023, VCC is notifying the one (1) Maryland resident whose information was known to have been potentially accessed without authorization. VCC is providing the notification via written letter sent by first-class United States mail. VCC has also arranged an offer for twelve (12) months of complimentary credit monitoring and identity theft protection services. Enclosed is a template copy of the notice that VCC will mail to the Maryland resident.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, VCC promptly initiated an internal investigation, notified local law enforcement, began restoring its systems from viable backups, and engaged a forensic firm to further investigate and secure its computer systems. In addition, VCC is reviewing its information security policies and evaluating additional trainings and controls it can implement to reduce the risk of a similar incident occurring in the future. Finally, as discussed above, VCC is notifying the individual whose personal information was potentially involved in the incident and is offering complimentary credit monitoring services.

CONTACT INFORMATION

Please do not hesitate to contact me if you have any questions or if I can provide you with any further information concerning this matter.

Sincerely,



Michael J. Waters

Enclosure



Excellence in Construction

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

RE: NOTICE OF A DATA BREACH

VCC, LLC values and respects the privacy of your information, which is why we are writing to advise you of an incident that involved some of your personal information. **While we have no reason to believe that your information has been misused for the purpose of committing fraud or identity theft**, we are writing in accordance with relevant law to advise you about the incident and to provide you with guidance on what you can do to protect yourself, should you feel it is appropriate to do so.

What Happened? On February 7, 2023, we learned of suspicious activity on our network. Upon discovering the incident, we promptly began an internal investigation, notified law enforcement, and engaged a forensic security firm to investigate and secure our computer systems. The investigation determined that an unknown third party accessed our systems on February 3, 2023, and that certain personal information was acquired as part of the incident.

What Information Was Involved? On March 15, 2023, we determined that the involved files contained some personal information, including your name and Social Security number, and for some people an address, date of birth, passport, driver's license or other government issued identification number, and health information, such as health insurance information, clinical or treatment information.

What We Are Doing. In addition to the actions described above, we have taken steps to reduce the risk of this type of incident occurring in the future, including enhancing our technical security measures. We are also offering a complimentary one-year membership of TransUnion (*myTrueIdentity*). This product helps detect possible misuse of your personal information and provides you with identity protection services focused on prompt identification and resolution of identity theft. TransUnion (*myTrueIdentity*) is completely free to you and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and TransUnion (*myTrueIdentity*), including instructions on how to activate your complimentary, one-year membership, please see the additional information attached to this letter.**

What You Can Do. We encourage you to take advantage of the complimentary credit monitoring included in this letter. You can also find more information on steps to protect yourself against possible identity theft or fraud in the *Additional Important Information* section below.

For More Information. We value the trust you place in us to protect your privacy, take our responsibility to safeguard your personal information seriously, and apologize for any inconvenience or concern this incident might cause. For further information and assistance, please call 888-572-8074 from 9:00 AM - 9:00 PM Eastern, Monday through Friday.

Sincerely,

VCC, LLC



Activation Code: <<Activation Code>>

3-Bureau Credit Monitoring Product Offering: (Online and Offline)

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service (*myTrueIdentity*) for **12 months** provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *myTrueIdentity* website at www.mytrueidentity.com and in the space referenced as “Enter Activation Code”, enter the following 12-letter Activation Code <<Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, three-bureau credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code [REDACTED] and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain **12 months** of unlimited access to your TransUnion credit report and credit score. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion, Experian and Equifax, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The subscription also includes access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the online or offline credit monitoring service anytime between now and <<**Enrollment Deadline**>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion®, Experian® and Equifax®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *myTrueIdentity* online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *myTrueIdentity* Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring 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. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

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

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 2000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate the freeze. A credit freeze can be placed without any charge and is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit 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 credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. As the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies below to find out more information:

Equifax Security Freeze
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.