BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Patrick H. Haggerty
direct dial: 513.929.3412
phaggerty@bakerlaw.com

July 13, 2023

VIA EMAIL (IDTHEFT@OAG.STATE.MD.US)

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

Re: Incident Notification

Dear Attorney General Brown:

We are writing on behalf of our client, Roots & Harvest Direct LLC ("R&H"), to notify your office of a cybersecurity incident experienced by one of their vendors, CommerceV3, which involved Maryland residents' information.

CommerceV3 provides an e-commerce platform R&H uses to process payment card information when an order is placed on the R&H websites. CommerceV3 learned that an unauthorized party obtained access to CommerceV3's systems between November 24, 2021 and December 14, 2022. Upon learning of this issue, CommerceV3 conducted a forensic investigation with third-party cybersecurity experts to assess whether cardholder data was involved in the incident. CommerceV3 also worked alongside the major card brands and banks during this forensic investigation.

On May 3, 2023, CommerceV3 discovered cardholder data it collected on R&H behalf was potentially accessed or acquired by an unauthorized party as a result of the incident. On June 6, 2023, CommerceV3 notified R&H of this incident. CommerceV3 and R&H worked to identify the individuals whose payment card information was involved in the incident and determined that it involved the names, email addresses, billing addresses, payment card numbers, card expiration dates, and card verification codes (CVV) for 54 Maryland residents.

On July 13, 2023, R&H will mail notification letters via United States Postal Service First-Class mail to the individuals whose information was involved, including the Maryland residents pursuant to Md. Code Ann., Com. Law § 14-3504. A copy of the notification is enclosed. R&H has established a dedicated call center for individuals to call with questions about the incident.

R&H understands that, to help prevent a similar incident from occurring in the future, CommerceV3 has implemented additional security measures.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Patrick H. Haggerty
Partner

Enclosure

PO Box 480149
Niles, IL 60714

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

July 13, 2023

Dear <<Name>> <<Name 2>>:

We write to notify you of an incident that impacted our third party e-commerce platform, CommerceV3, that may have involved some of your payment card information. We are writing to provide you with information regarding the incident and steps you can take in response.

Why Does CommerceV3 Have My Information?
CommerceV3 provides the e-commerce platform we use to process payment card information when an order is placed on our website. This incident occurred at CommerceV3 and not at Roots & Harvest Direct LLC.

What Happened?
CommerceV3 learned that an unauthorized party obtained access to its systems between November 24, 2021 and December 14, 2022. Immediately upon learning of this issue, CommerceV3 conducted a thorough forensic investigation alongside third-party cybersecurity experts to assess whether any cardholder data was involved. CommerceV3 also worked alongside the major card brands and banks during this forensic investigation.

What We Are Doing.
On May 3, 2023, after an extensive forensic investigation, CommerceV3 discovered that cardholder data collected on Roots & Harvest Direct LLC's behalf was potentially accessed and/or acquired by an unauthorized party as a result of the incident. CommerceV3 notified Roots & Harvest Direct LLC of this incident on June 6, 2023. We then worked with CommerceV3 to identify the individuals whose payment card information was involved. In response to the incident, CommerceV3 has implemented additional security measures.

What Information Was Involved?
The information that was potentially accessed and/or acquired as a result of this incident included your name, email address, billing address, payment card number ending in <<Variable Text>>, card expiration date, and the card verification code (CVV).

What You Can Do.
We encourage you to remain vigilant by reviewing your payment card account statement. If you see charges or activity that you did not authorize, contact your payment card company immediately. The telephone number is on the back of your payment card. Please review the following pages for more information on ways to protect yourself.

For More Information.
If you have any further questions regarding this incident, please call 1-888-220-4902. This response line is available Monday through Friday, 9 am – 9 pm Eastern Time.

Sincerely,

Ashley Kohnen
Roots & Harvest Direct LLC

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 1000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts and Security Freezes

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- *Equifax Security Freeze*, PO Box 105788, Atlanta, GA 30348, www.equifax.com
- *Experian Security Freeze*, PO Box 9554, Allen, TX 75013, www.experian.com
- *TransUnion Security Freeze*, PO Box 160, Woodlyn, PA 19094, www.transunion.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Roots & Harvest Direct LLC can be reached at 877-336-5895. Its mailing address is 4440 Muhlhauser Rd. Suite 300, West Chester, OH 45011-9767.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves <<XX>> individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.