Appendix

On February 23, 2021, NOCO received information from the Department of Homeland Security that payment card numbers for sale on the dark web had NOCO as a common point of purchase (CPP). Upon learning this, NOCO retained Baker & Hostetler, LLP to provide legal advice and assistance investigating and responding to the incident. BakerHostetler then engaged a cybersecurity investigator to conduct a forensic review to assist BakerHostetler in providing legal advice to NOCO.

On March 23, 2021, the forensic investigation identified malicious code on NOCO's website and the code was removed. The function of the code was analyzed, and on April 8, 2021, NOCO learned that the code permitted an unauthorized party to copy information entered onto the website, no.co, including individuals' names, usernames and passwords for accessing accounts on no.co and credit or debit card numbers. The investigation determined that an unauthorized party may have copied this information, as entered on to the website, between October 8, 2019 and March 23, 2021. On April 15, 2021, NOCO identified contact information for the individuals whose information was potentially accessed and determined that 24 Maine residents' information was included in the accessible data.

On May 18, 2021, NOCO will begin mailing notification letters to the Maine residents.[1] A sample copy of the notification letter is attached. NOCO is recommending that all individuals review their account statements and credit reports for any unauthorized activity and report any unauthorized charges or activity immediately. NOCO has also established a dedicated, toll-free call center where individuals may obtain more information regarding the incident.

To help prevent something like this from happening again, NOCO has updated passwords and implemented additional security safeguards and controls on its website. After the discovery of the incident, all payments were routed to occur solely on Amazon or PayPal until all security enhancements on the website are or have been completed.

[1] This report does not waive NOCO's objection that Maine lacks personal jurisdiction over it related to any claims that may arise from this incident.

The NOCO Company
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

First Name Last Name D-1
Address 1
Address 2
City, State, Zip

May 17, 2021

Dear First Name Last Name:

The NOCO Company understands the importance of protecting our customers' information. We are writing to inform you of an incident that may have involved some of your information. We are providing this notice to explain the incident and measures we have taken, and also to provide some steps you can take in response.

On March 23, 2021, we identified malicious code on our website, which we promptly removed. With the assistance of a cybersecurity firm, we investigated the purpose of the malicious code. On April 8, 2021, we learned that the malicious code permitted an unauthorized party to access information entered onto our website, no.co, including payment card information.

The investigation determined that an unauthorized party may have accessed payment card information entered onto our website between October 8, 2019 and March 23, 2021. We reviewed the transactions from our website and determined that you made a purchase on the site during that time period. The information that was accessible includes your name, username, and password for accessing your account on noco.com and your credit or debit card number ending in xxxx.

In response to the incident, we have taken steps to help prevent a similar incident in the future including updating user passwords and implementing additional security safeguards and controls on our website. We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. If you see charges or activity, you did not authorize, please contact the relevant financial institution or credit bureau reporting the activity immediately. For more information, including some additional steps you can take to help protect yourself, please see the additional information provided with this letter.

If you have any questions, please call 844-502-9994, Monday through Friday, 9:00 a.m. to 6:00 p.m. Eastern Time.

Sincerely,

The NOCO Company

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, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, 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.ftc.gov/idtheft

Fraud Alerts and Credit or 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:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.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.

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 22 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.