BakerHostetler

Baker&Hostetler LLP

1900 Avenue of the Stars
Suite 2700
Los Angeles, CA 90067-4508

T 310.820.8800
F 310.820.8859
www.bakerlaw.com

April 16, 2024

VIA E-MAIL (DOJ-CPB@DOJ.NH.GOV)

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Formella:

We are writing on behalf of our client, Cocoon Inc. ("Cocoon"), to notify your office of a security incident.

A vendor that manages Cocoon's network experienced a cybersecurity incident involving malware, which encrypted some of Cocoon's systems on March 4, 2024. Cocoon immediately began an investigation, a cybersecurity firm was engaged, and measures were taken to address the incident and to restore systems. Through its investigation, Cocoon learned that there was unauthorized activity in its network between March 3, 2024 and March 7, 2024. During that time, an unauthorized party accessed files stored on Cocoon servers. Cocoon launched a review of the potentially accessed files to determine whether the incident involved any personal information. On March 27, 2024, Cocoon identified files that contained the . Cocoon then worked to identify addresses for the individuals whose information was involved, including twenty five (25) New Hampshire residents.

On April 11, 2024, Cocoon began mailing and hand delivering notification letters to the New Hampshire residents in accordance with N.H. Rev. Stat. Ann. § 359-C:20. A copy of the notification letter is enclosed. Cocoon is providing a telephone number for notified individuals to call with any questions they may have about the incident. Cocoon is offering notified individuals a complimentary membership to credit monitoring and identity protection services.

To help prevent this type of incident from happening again, Cocoon has implemented additional measures to enhance its existing security protocols.

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

Sincerely,

M. Scott Koller
Partner

Enclosure

<<Name 1>> <<Name 2>>

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

<<Date>>

Dear <<Name 1>>:

We are writing to inform you of an incident that may have involved some of your information. This letter explains the incident and measures we have taken, and provides some steps you can take in response.

What Happened?
A vendor that manages Cocoon's network experienced a cybersecurity incident involving malware, which encrypted some of Cocoon's systems on March 4, 2024. Upon detection, we quickly took steps to secure our network and launched an investigation with the assistance of cybersecurity professionals. Our forensic investigation has determined that an unauthorized party obtained access to certain data that was stored on our systems.

What Information Was Involved?
We reviewed the data that was potentially accessed during the vendor incident and, on March 27, 2024, determined that select servers encrypted by the malware contained documents that may have included your

.

What Are We Doing?
Your confidence and trust are important to us, and we regret any inconvenience or concern this incident may cause. To further protect your information, we have implemented additional measures to enhance our existing security protocols. Additionally, in an abundance of caution, we have arranged to provide identity monitoring at no cost to you through IDX. IDX identity protection services include: of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

What You Can Do.
It is always a good idea to remain vigilant by regularly reviewing your financial accounts and credit reports for any unauthorized activity. We also encourage you to enroll in IDX's identity monitoring service. For more information on identity theft prevention and your complimentary services, as well as some additional steps you can take to protect your personal information, please see the additional pages enclosed with this letter.

For More Information.
We regret any inconvenience or concern this incident may cause and take this matter seriously. If you have any questions, please call X-XXX-XXX-XXXX, Monday through Friday, 8:00 a.m. to 5:00 p.m. Eastern Time.

Sincerely,

Ray Gaffey
Chief Operating Officer, Cocoon Inc.

ENROLLMENT INSTRUCTIONS

1. **Website and Enrollment.** Go to <<URL>> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is .

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at X-XXX-XXX-XXXX to speak with knowledgeable representatives for enrollment assistance.

If you discover any suspicious items and have enrolled in IDX identity protection, notify IDX immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of IDX's ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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 over the next 12 to 24 months. 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.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 160 Woodlyn, PA 19094, 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.

Cocoon Inc. is located at 216 Lafayette Road, North Hampton, New Hampshire 03862,

Additional information for residents of the following states:

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 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