

Kirk J. Nahra

+1 202 663 6128 (t)
+1 202 663 6363 (f)
kirk.nahra@wilmerhale.com

November 6, 2023

VIA U.S. MAIL

Attorney General Anthony Brown
200 St. Paul Place
Baltimore, MD 21202-2202

Re: *Incident Notification*

To Whom It May Concern:

I am writing on behalf of our client, Cartiga LLC (“Cartiga”), to provide notice to your office concerning a security incident involving four (4) Maryland residents. Cartiga, which is located at 400 Park Avenue, NY, NY 10022, provides funding solutions to attorneys and their clients.

On or around March 20, 2023, Cartiga discovered that one of its corporate laptops had been compromised through a phishing attack. As soon as Cartiga became aware of the situation, it quickly and thoroughly conducted an investigation to understand which components of Cartiga’s systems were impacted.

There is no evidence of any continuing unauthorized activity in relation to this incident, and we currently do not have any evidence that any personal information has been used for any fraudulent or illicit purposes. Based on the company’s investigation to date, the affected consumer personal information included names, addresses, dates of birth, health information, social security numbers, or other identification numbers (such as driver’s license numbers).

Cartiga mailed notifications to affected individuals on November 6, 2023. An example of the notification mailed to Maryland residents is attached. As the sample letter indicates, we are also providing all affected individuals with 24 months of free credit monitoring.

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

Attorney General Brown
November 6, 2023
Page 2

WILMERHALE

Sincerely,

Kirk Nahra

Kirk Nahra

Enclosure



Return: P.O. Box 3826
Suwanee, GA 30024

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

<<Maildate>>

Re: Notice of Data Breach

Dear <<Name 1>>:

We are writing to notify you of a security incident involving Cartiga, LLC (“Cartiga,” “us,” “our,” or “we”) that impacted some of the personal information you provided to us as part of engaging with our services. We deeply regret that this incident occurred despite our significant and ongoing investment in data security.

This letter provides details about the incident, explains how we are prepared to assist you, and informs you of what steps we are taking to continue to protect your personal information.

What Happened?

On or around March 20, 2023, Cartiga discovered that one of its corporate laptops had been compromised through a phishing attack. As soon as we became aware of the situation, we quickly and thoroughly conducted an investigation to understand which components of Cartiga’s systems were impacted. The investigation determined that some of your personal information may have been compromised as a result of this incident.

Please note that there is no evidence of any continuing unauthorized activity in relation to this incident, and we currently do not have any evidence that your personal information has been used for any fraudulent or illicit purposes.

What Information Was Involved?

Information that could potentially have been accessed may include your name, address, date of birth, health information, your social security number, and other identification numbers (such as your driver’s license number).

What We Are Doing

We take privacy and the protection of the information in our possession very seriously, and we worked swiftly to investigate and to resolve this incident. We have conducted a thorough review of the potentially affected records and are implementing additional security measures, internal controls, and safeguards, as well as making changes to our policies and procedures to prevent a similar occurrence in the future.

Additionally, as a precaution to help protect your identity, we are providing 24 months of identity theft prevention and mitigation services, including credit monitoring at no cost to you. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by:** <<enrollment deadline>> (Your code will not work after this date.)
- Go to [REDACTED].
- Enter your unique Activation Code of << Activation Code >> then click “Submit” and follow these 4 steps:
 1. **Register:** Complete the form with your contact information and click “Continue”. If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
 2. **Create Account:** Enter your email address, create a password, and accept the terms of use.
 3. **Verify Identity:** To enroll in your product, we will ask you to complete our identity verification process.
 4. **Checkout:** Upon successful verification of your identity, you will see the Checkout Page. Click ‘Sign Me Up’ to finish enrolling. You’re done! The confirmation page shows your completed enrollment. Click “View My Product” to access the product features.

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling online, please contact the customer care team at [REDACTED] by <<enrollment deadline>>.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EQUIFAX CREDIT WATCH GOLD:

A credit card is **not** required for enrollment.

You have access to the following features once you enroll in Equifax Credit Watch Gold:

- **Credit monitoring with email notifications** of key changes to your Equifax credit report;
- **Daily access** to your Equifax credit report;
- **WebScan notifications**¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites;
- **Automatic fraud alerts**², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- **Identity Restoration** to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf;

¹ WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

² The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

³ Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com

- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft.⁴

What You Can Do

To further protect your information, you can take steps to monitor your accounts, obtain your credit reports, or place a fraud alert or security freeze on your credit account. For information on each of these steps, please review **Attachment A**. Depending on your jurisdiction, you may also have additional rights available to you, which you can review in **Attachment B**.

For More Information

On behalf of the entire Cartiga team, we sincerely regret that this incident occurred. Should you have any questions, please do not hesitate to call [REDACTED], anytime from 9am – 9pm EST, Monday through Friday.

Sincerely,
Cartiga, LLC

⁴ The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Attachment A: Additional Information on Protecting Your Information

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®

P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian

P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®

P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit 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 a freeze. A credit freeze 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 access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax®

P.O. Box 105788
Atlanta, GA 30348-5788
1-888-378-4329
www.equifax.com/personal/credit-report-services/credit-freeze/

Experian

P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion®

P.O. Box 160
Woodlyn, PA 19094-0160
1-888-916-8800
www.transunion.com/credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- 1) Full name, with middle initial and any suffixes;
- 2) Social Security number;
- 3) Date of birth (month, day, and year);
- 4) Current address and previous addresses for the past five (5) years;
- 5) Proof of current address, such as a current utility bill or telephone bill;
- 6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax®

P.O. Box 105069
Atlanta, GA 30348-5069
1-888-378-4329
[www.equifax.com/personal/
credit-report-
services/credit-fraud-alerts/](http://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/)

Experian

P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
[www.experian.com/
fraud/center.html](http://www.experian.com/fraud/center.html)

TransUnion®

P.O. Box 2000
Chester, PA 19016-2000
1-800-916-8800
www.transunion.com/fraud-alerts

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission

600 Pennsylvania Avenue
NW Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

Attachment B: Additional State Law Information

For residents of the District of Columbia, Iowa, Maryland, New York, North Carolina, Oregon and Rhode Island

You may contact your Attorney General for additional information about avoiding identity theft. If you are a Rhode Island resident, you may also file a police report by contacting local or state law enforcement agencies. You may use the following information to contact your attorney general:

Maryland Office of the Attorney General Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202 (410) 528-8662 www.marylandattorneygeneral.gov	New York Attorney General Consumer Frauds & Protection Bureau 120 Broadway, 3rd Floor New York, NY 10271 (800) 771-7755 www.ag.ny.gov	New York Department of State Division of Consumer Protection 99 Washington Avenue Suite 650 Albany, New York 12231 (800) 697-1220 www.dos.ny.gov
North Carolina Department of Justice 9001 Mail Service Center Raleigh, NC 27699-9001 (919) 716-6000 www.ncdoj.gov	Oregon Department of Justice 1162 Court Street NE Salem, OR 97301-4096 (877) 877-9392 www.doj.state.or.us	Rhode Island Office of the Attorney General Consumer Protection Division 150 South Main Street Providence, RI 02903 (401) 274-4400 www.riag.ri.gov

For residents of Massachusetts: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of New Mexico: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov.