

July 2, 2021

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Online Portal

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: Cybersecurity Incident Involving GPCD Partners, LLC.

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents GPCD Partners, LLC (“GPCD”), an accounting firm located in Philadelphia, Pennsylvania, with respect to a recent cybersecurity incident that was first discovered by GPCD on April 5, 2021 (hereinafter, the “Incident”). GPCD takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

Although GPCD will provide notice to the affected individuals pursuant to state law, GPCD wanted to inform you as soon as possible of the Incident given it received confirmation of 3 potentially impacted Maine residents.

1. Nature of the Incident.

On April 5, 2021, GPCD became aware of a suspicious activity related to one of GPCD employee’s computer. Upon discovery of this incident, GPCD promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Based on the investigation, it was determined that some sensitive personal information may have been accessed by an unauthorized individual. Therefore, GPCD worked to identify the specific individuals and the type of information that may have been compromised in order to send out notice of the Incident to these individuals. At this time, we have no reason to believe that the personal information has been misused by any third parties.

The information involved may have included the individuals’ names, addresses, dates of birth, social security numbers, driver’s license numbers, taxpayer identification numbers, financial account information, W-2 wage statements, and tax statements. Again, at this time, we have no reason to believe that their personal information has been misused by any third parties. But out of an abundance of caution, we wanted to inform you of this Incident.

2. Number of Maine residents affected.

GPCD identified 1,591 clients who were potentially affected by this Incident. Of those 1,591 clients, 3 were Maine residents. Pursuant to state law, individual notification letters were mailed on July 2, 2021, by first class mail. A sample copy of the notification letter being mailed to the potentially affected residents of Maine is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

GPCD takes the security and privacy of all client information very seriously, and has taken steps to protect the privacy and security of potentially impacted individuals' information. Specifically, upon discovery of this Incident, GPCD changed all passwords, wiped and re-formatted every computer, installed network protection programs, and installed Carbon Black, an endpoint monitoring and detection tool, to continuously monitor for any malicious activity within its systems. GPCD also launched a forensic investigation to determine the full nature and scope of this incident. Lastly, GPCD informed our law firm and began identifying the affected individuals in preparation for notice.

As outlined in the sample notification to the impacted individual, GPCD provided the impacted individuals with complimentary services to help protect their identity. Specifically, GPCD has arranged for the impacted individuals to enroll in identity monitoring services (including identity theft protection) provided by Kroll at no cost to them for 12 months.

4. Contact information.

GPCD remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Anjali C. Das

Enclosure

Exhibit A

GPCD PARTNERS, LLC

CERTIFIED PUBLIC ACCOUNTANTS

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

GPCD Partners, LLC (“GPCD”) is writing to inform you of a recent data security incident that may have resulted in the disclosure of your personal information. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with details about the event, steps we are taking in response, and resources available to help you protect yourself from the possibility of identity theft and fraud, should you feel it is appropriate to do so.

What Happened?

On April 5, 2021, GPCD became aware of a suspicious activity related to one of GPCD employee’s computer. Upon discovery of this incident, GPCD promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. Based on the investigation, it was determined that some sensitive personal information may have been accessed by an unauthorized individual. Therefore, GPCD worked to identify the specific individuals and the type of information that may have been compromised in order to send out notice of the incident to these individuals. At this time, we have no reason to believe that your personal information has been misused by any third parties. But out of an abundance of caution, we wanted to inform you of this incident.

What Information Was Involved?

The information involved may have included your name, address, date of birth, social security number, driver’s license number, taxpayer identification number, financial account information, W-2 wage statements, and tax statements. Again, at this time, we have no reason to believe that your personal information has been misused by any third parties. But out of an abundance of caution, we wanted to inform you of this incident.

What We Are Doing

We are committed to ensuring the security of all personal information in our control. The privacy of the people we provide services to is very important to us and we will continue to do everything we can to protect it. Upon discovery of this incident, we changed all passwords, wiped and re-formatted every computer, installed network protection programs, and installed Carbon Black, an endpoint monitoring and detection tool, to continuously monitor for any malicious activity within our systems. We also launched a forensic investigation to determine the full nature and scope of this incident.

Out of an abundance of caution, we are also providing you with 12 months of complimentary identity monitoring services through Kroll, as well as, guidance on how to help protect against the possibility of information misuse. While we are covering the cost of these services, you will need to complete the activation process by following the instructions included in the enclosed *Steps You Can Take to Help Protect Your Information*.

At this time, we are not aware of your information being used in an unauthorized manner, but out of an abundance of caution, we wanted to make you aware of this matter and offer resources to help protect your information.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse. You may also activate the identity monitoring services we are making available to you. Again, we are making these services available to you at no cost; however, you will need to activate these services.

In addition, security experts suggest that you contact your financial institution and all major credit bureaus immediately to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

We recognize that you may have questions not addressed in this letter. Should you any questions or concerns about this incident, please contact 1-855-731-3355 (toll free) between the hours 8:00 a.m. and 5:30 p.m. Central Standard Time, Monday through Friday (excluding U.S. national holidays) for more information.

We sincerely regret any inconvenience that this matter may cause, and remain dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

A handwritten signature in black ink, appearing to read "John C. Papandon". The signature is fluid and cursive, with a large initial "J" and a long, sweeping underline.

John C. Papandon, Esq., CPA, LLM
Partner
GPCD Partners, LLC

Steps You Can Take to Help Protect Your Information

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until **September 28, 2021** to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Additional Important Information

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

<p>Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html</p>	<p>TransUnion P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts</p>	<p>Equifax P.O. Box 105069 Atlanta, GA 30348 1-888-525-6285 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/</p>
--	--	--

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies listed above.

<p>Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html</p>	<p>TransUnion P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze</p>	<p>Equifax P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 https://www.equifax.com/personal/credit-report-services/credit-freeze/</p>
--	---	---

More information can also be obtained by contacting the Federal Trade Commission:

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

For residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming:* It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Colorado, Illinois, Iowa, Maryland, Missouri, New Mexico, North Carolina, Oregon, and West Virginia:* It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa:* State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *New Mexico:* State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

For residents of *Oregon:* State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island:* You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

District of Columbia Office of the Attorney General - 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov

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

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report filed in regard to this 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 *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.