



August 30, 2022

BY EMAIL

Office of the Attorney General
200 St. Paul Plaza
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

On behalf of Platinum Performance, Inc. ("Platinum"), and pursuant to Md. Code Ann., Com. Law § 14-3504(h), this letter provides notice of a cybersecurity incident involving Maryland residents. By way of background, Platinum is a nutrition-focused health company headquartered in Buellton, CA that offers veterinary-developed nutritional supplements for animals and people.

On May 6, 2022, Platinum discovered unauthorized access by a third-party to the email mailboxes of two employees and promptly initiated our Cybersecurity and Privacy Incident Response Plans, which included engaging third-party forensic experts to conduct an investigation. The investigation revealed that the unauthorized access began on September 8, 2021 as a result of an email phishing incident. The incident was discovered and remediated on May 6, 2022. Investigation conducted through July and August revealed that personal data was contained in the compromised email accounts and may have been available to the unauthorized third party. This matter has been reported to the FBI, but this notification was not delayed as a result of any law enforcement investigation.

To date, we have determined that six (6) Maryland residents may have been affected. Depending on the individual, the types of personal information that may have been affected included Social Security number, financial account number, or credit or debit card information. As of the time of writing, Platinum is not aware of any misuse of consumer personal information as a result of the incident.

Platinum anticipates sending these individuals formal notice on August 31, 2022 via U.S. first class mail. A sample of the notification letter is enclosed. As stated in the attached sample notice, Platinum is offering to provide individuals 24 months of free identity theft monitoring services through Kroll. Platinum's internal customer care center will respond to questions from notified individuals.

Platinum has enhanced its internal security measures to help prevent a similar incident from happening in the future. We have implemented multi-factor authentication for all external accounts and implemented a new email security gateway to help ensure phishing campaigns are effectively blocked and quarantined. We are also providing additional training to our employees on cybersecurity preparedness and incident response.

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

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

NOTICE OF SECURITY INCIDENT

Dear <<first_name>>,

We are writing to inform you about a cyber security incident affecting Platinum Performance, Inc. ("Platinum") that may have affected some of your personal information. We take the privacy of your information very seriously and we sincerely regret any inconvenience or concern this incident may cause. This notice outlines some steps you may take to help protect your information. We understand this can be concerning, and we want to help guide you through the process and navigate the appropriate actions to take.

Keeping personal data safe and secure is very important to us and will continue to be a priority for Platinum moving forward.

WHAT HAPPENED?

Platinum discovered unauthorized access by a third-party to the email mailboxes of two employees on May 6, 2022 and promptly initiated our Cybersecurity and Privacy Incident Response Plans, which included engaging third-party forensic experts to conduct an investigation. The investigation revealed that the unauthorized access occurred on September 8, 2021, as a result of an email phishing incident. Further investigation through July and August revealed that your personal data was contained in one of the two compromised email accounts and may have been available to the unauthorized third party.

WHAT INFORMATION WAS INVOLVED?

The personal information that may have been affected includes <<b2b_text_1 (data elements)>>. As of the time of writing, we have no information suggesting that your personal information has been misused as a result of this incident.

WHAT WE ARE DOING

We took steps to address and contain the incident the same day it was discovered. As previously mentioned, we promptly engaged third-party forensic experts to investigate the incident. We have also notified law enforcement of this incident but have not delayed this notification as a result of any law enforcement investigation. Platinum has enhanced our internal security measures to help prevent a similar incident from happening in the future.

To assist you in monitoring your personal data, we have also secured the expert services of Kroll, a global leader in risk mitigation and response, to provide identity monitoring services at no cost to you for two years. Your identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

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

You have until <<b2b_text_6 (date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

WHAT YOU CAN DO

We encourage you to take advantage of the identity monitoring services we are providing to you free of charge. In addition, you should remain vigilant and carefully review your accounts for any suspicious activity. This is a best practice for all consumers. Included below are some additional helpful tips and steps you can take to help protect your information against the risks of fraud and identity theft.

- **Data Security:** Practice good data security by ensuring your computer has up-to-date anti-virus protection and updating your passwords regularly and ensuring they are complex and unique.
- **Email Information:** Pay particular attention to any emails asking for personal data, financial information, or government identifiers. Please do not give out your Social Security number or other personal data to unknown sources.
- **Fraudulent Messages:** Always remain alert to phishing scams. Phishing scams involve fraudulent (i.e., fake or “spoofed”) email messages that appear to come from legitimate sources and encourage you to (i) click on a link or open an attachment that will download malware onto your computer, or (ii) provide an unknown third party with certain types of information. For example, you may receive an email that directs you to input information, such as your username and password, into an unauthorized website. You may also receive an email from a source that appears to be legitimate but may be off in some way. An email may also be a phishing scam if it has certain anomalies, such as misspellings or awkward phrasing.
- **Review Bank Statements:** Review your credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. You should remain vigilant and continue to monitor your statements for unusual activity going forward. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.
- **Credit Reports:** Carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately.

If you would like to take additional steps to help protect your personal information, attached to this letter are helpful resources on how to do so, including recommendations from the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

FOR MORE INFORMATION

If you have any questions, please contact us at 800-553-2400, Monday through Friday from 6:00 a.m. to 5:00 p.m. Pacific Time, excluding major U.S. holidays. We understand this incident is inconvenient and we are here to help lead you through the next steps to protect your personal information.

Sincerely,

Platinum Performance

Additional Resources

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. 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 law enforcement, the Federal Trade Commission (“FTC”) and/or the Attorney General’s office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

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

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <https://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at <https://www.annualcreditreport.com/manualRequestForm.action>. Credit reporting agency contact details are provided below.

Equifax:

equifax.com
equifax.com/personal/credit-report-services
P.O. Box 740241
Atlanta, GA 30374
866-349-5191

Experian:

experian.com
experian.com/help
P.O. Box 2002
Allen, TX 75013
888-397-3742

TransUnion:

transunion.com
transunion.com/credit-help
P.O. Box 1000
Chester, PA 19016
888-909-8872

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

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: 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; and you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Additional Information

You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado, Delaware, and Illinois residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, <http://www.marylandattorneygeneral.gov>, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, <http://www.ncdoj.gov>, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.

For Georgia, Maryland, New Jersey, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

For New York residents: You may contact the New York Office of the Attorney General at: The Capitol, Albany, NY 12224-0341, <http://www.ag.ny.gov/home.html>, 1-800-771-7755, and the New York Department of State Division of Consumer Protection at: 99 Washington Avenue, Albany, New York 12231-0001, <http://www.dos.ny.gov/consumerprotection>, 1-800-697-1220.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will 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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.