



David McMillan, Partner  
Cybersecurity & Data Privacy Team  
175 Pearl Street, Suite C-402  
Brooklyn, NY 11201  
dmcmillan@constangy.com  
Mobile: 718.614.8371

November 12, 2024

**VIA EMAIL**

Attorney General Anthony Brown  
Office of the Attorney General  
ATTN: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202  
idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy Brooks Smith & Prophete LLP represents Mandrake Capital Partners LLC ("Mandrake") in connection with a recent data security incident described in greater detail below.

**1. Nature of the security incident.**

On September 23, 2024, Mandrake began seeing unusual activity in its IT environment that was confirmed to be the result of a malicious encryption attack. Upon discovering this activity, Mandrake immediately took steps to secure the environment and engaged independent cybersecurity experts to investigate and help to determine whether any data within the network was affected. Based on the investigation, Mandrake determined that an unauthorized actor gained access to its servers and potentially downloaded certain data from the network. After reviewing this data in detail, on October 28, 2024, Mandrake learned that certain personal information was affected by the incident.

Mandrake then worked diligently to identify current address information for purposes of promptly providing notification. Importantly, Mandrake has no evidence of the misuse or attempted misuse of any potentially impacted information.

The information that may have been affected by this incident varies by individual, but includes individuals' names, driver's license numbers, passport numbers, and/or Social Security numbers.

**2. Number of Maryland residents notified.**

Mandrake notified one (1) Maryland resident of this incident via first class U.S. mail on November 12, 2024. A sample copy of the notification letter is included with this correspondence.

**3. Steps taken relating to the Incident.**

As soon as Mandrake discovered this incident, it took steps to secure its environment and launched an investigation to determine whether personal information had been accessed or acquired without authorization. Mandrake has also implemented additional safeguards to help ensure the security of its environment and to reduce the risk of a similar incident occurring in the future.

November 12, 2024

Page 2

Mandrake has established a toll-free call center through TransUnion, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. In addition, while Mandrake is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, Mandrake is also providing complimentary identity protection services to all notified individuals.

**4. Contact information.**

Mandrake remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me.

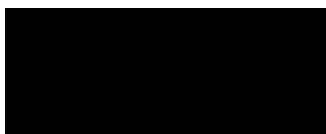
Sincerely,

A handwritten signature in black ink, appearing to read "D. McMillan", followed by a horizontal line extending to the right.

David McMillan  
Partner, Cybersecurity & Data Privacy Team

Enclosure: Sample Notification Letter

Mandrake Capital Partners LLC  
c/o Cyberscout  
PO Box 1286  
Dearborn, MI 48120-9998



November 12, 2024

**Subject: Notice of Data Security Incident**

Dear :

I am writing to inform you about a recent data security incident experienced by Mandrake Capital Partners LLC ("Mandrake") that may have affected your personal information. Please read this carefully as it contains details about the incident and resources you can utilize to help protect your information, including instructions for enrolling in complimentary credit monitoring and identity restoration services.

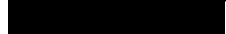
**What Happened:** On September 23, 2024, Mandrake began seeing unusual activity in its IT environment which was confirmed to be the result of a malicious encryption attack. Upon discovering this activity, we immediately took steps to secure the environment and engaged independent cybersecurity experts to investigate what happened and help us determine whether any data within our network was affected. Based on the investigation, we determined that an unauthorized actor gained access to our servers and potentially downloaded certain files containing investor information. After reviewing those files in detail, on October 28, 2024, we learned that your personal information was included within the potentially impacted files which is the reason for this notification.

**What Information Was Involved:** The information that may have been downloaded by unauthorized party includes your name as well as your Social Security number. Please note that Mandrake has no evidence that any of this information has been misused.

**What We Are Doing:** As soon as we learned of the incident, we took the measures described above and implemented additional security features to reduce the risk of a similar incident occurring in the future. We also reported the incident to federal law enforcement and will offer any assistance we can to help hold the perpetrators accountable.

In addition, we are providing you with the opportunity to enroll in Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge to you. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted, please provide the following unique code to receive services:



To receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account, and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

000010102G0500

P

**What You Can Do: What You Can Do:** We encourage you to enroll in the complementary services being offered to you through Cyberscout by using the enrollment information provided above. You can also follow the recommendations on the following page to help protect your personal information.

**For More Information:** Representatives are available for 90 days from the date of this letter to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-800-405-6108 and supply the specialist with your unique code listed above.

Mandrake takes this situation extremely seriously as the privacy and protection of our investors' information is a top priority. We appreciate your understanding and apologize for any inconvenience or worry this may cause.

Sincerely,

A handwritten signature in dark ink, appearing to read "Michael Kavourias". The signature is fluid and cursive, with the first name "Michael" and last name "Kavourias" clearly distinguishable.

Michael Kavourias  
Mandrake Capital Partners LLC  
300 Park Avenue, Suite 1202  
New York, NY 10022

## Steps You Can Take to Protect Your Personal Information

**Review Your Account Statements and Notify Law Enforcement of Suspicious Activity:** As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

**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 <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

**Equifax**  
P.O. Box 105851  
Atlanta, GA 30348  
1-800-525-6285  
[www.equifax.com](http://www.equifax.com)

**Experian**  
P.O. Box 9532  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

**TransUnion**  
P.O. Box 1000  
Chester, PA 19016  
1-800-916-8800  
[www.transunion.com](http://www.transunion.com)

**Fraud Alert:** You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

**Security Freeze:** You have the right to put a security freeze on your credit file for up to one year at no cost. 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 potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. 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 insurance statement.

**Additional Free Resources:** You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

**Federal Trade Commission**  
600 Pennsylvania Ave, NW  
Washington, DC 20580  
[consumer.ftc.gov](http://consumer.ftc.gov)  
877-438-4338

**Maryland Attorney General**  
200 St. Paul Place  
Baltimore, MD 21202  
[www.marylandattorneygeneral.gov/Pages/CPD](http://www.marylandattorneygeneral.gov/Pages/CPD)  
888-743-0023

**California Attorney General**  
1300 I Street  
Sacramento, CA 95814  
[www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)  
800-952-5225

**New York Attorney General**  
The Capitol  
Albany, NY 12224  
800-771-7755  
[ag.ny.gov](http://ag.ny.gov)

**NY Bureau of Internet and Technology**  
28 Liberty Street  
New York, NY 10005  
[www.dos.ny.gov/consumerprotection/](http://www.dos.ny.gov/consumerprotection/)  
212.416.8433

**Washington D.C. Attorney General**  
400 S 6th Street, NW  
Washington, DC 20001  
[oag.dc.gov/consumer-protection](http://oag.dc.gov/consumer-protection)  
202-442-9828



00001020280000

P

**You also have certain rights under the Fair Credit Reporting Act (FCRA):** These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit

<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>