



Laura K. Funk, Partner
Cybersecurity & Data Privacy Team
100 Crescent Court, Suite 700
Dallas, Texas 75201
LFunk@constangy.com
Mobile: 248.709.9385

March 21, 2025

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: Notification of Data Security Incident

Dear Attorney General Brown:

Constangy Brooks Smith & Prophete LLP represents NewAgeSys Inc. ("NewAgeSys"), located in Princeton, New Jersey, with respect to a data security incident described in greater detail below. The purpose of this letter is to notify you of the incident.

Nature of the Security Incident

In March 2024, NewAgeSys experienced an encryption incident that disrupted access to certain parts of its digital environment. In response, it took immediate steps to secure its environment and promptly launched an investigation. As a result of this investigation, NewAgeSys learned that an unauthorized actor acquired certain data stored in its systems. After a thorough review of the data, on February 24, 2025, NewAgeSys determined that certain personal information may have been impacted by this incident.

The affected information includes individuals' names and Social Security numbers.

Number of Maryland Residents Affected

On March 21, 2025, NewAgeSys notified ninety (90) Maryland residents of this incident via First-Class U.S. Mail. A sample copy of the notification letter sent to impacted individuals is included with this correspondence.

Steps Taken Relating to the Incident

To help prevent something like this from happening again, NewAgeSys is implementing additional security protocols. It is also offering complimentary credit and identity protection monitoring services to all notified individuals.

Contact Information

NewAgeSys remains dedicated to protecting the information in its possession. If you have any questions or need additional information, please do not hesitate to contact me by email at lfunk@constangy.com.

Regards,

A handwritten signature in black ink, appearing to read 'L. Funk', with a long, sweeping horizontal line extending to the right.

Laura K. Funk
Partner

Enc.: Sample Consumer Notification Letter

NewAgeSys Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

NewAgeSys



March 21, 2025

Subject: Notice of Data Security Incident

Dear [REDACTED]:

We are writing to inform you of a data security incident experienced by NewAgeSys Inc. (“NewAgeSys”), located in Princeton, New Jersey, that may have involved some of your information. This letter is to notify you of the incident, offer you complimentary identity protection services, and inform you about steps you can take to help protect your personal information.

What Happened. On February 24, 2025, NewAgeSys learned that some of your personal information was involved in a data security incident. NewAgeSys experienced an encryption incident that disrupted access to certain parts of our network in March 2024. In response, we began an investigation and took steps to secure our network. During the investigation, we learned that certain data stored on our systems was acquired without authorization during the incident. We then worked to identify all potentially affected data and conducted a thorough review of that data to determine whose information was potentially involved. Please note that we have no evidence of the misuse of anyone’s information.

What Information Was Involved. The data that was acquired without authorization included your name and Social Security Number.

What We Are Doing. To help prevent something like this from happening again, we have implemented additional technical security measures to enhance the security of our network. In addition, we are also providing you with information about steps that you can take to help protect your personal information and offering you [REDACTED] months of complimentary identity monitoring services through Cyberscout, a TransUnion company. This service helps detect possible misuse of your information and provides you with identity protection support.

What You Can Do. For more information on how you can protect your personal information, please review the resources provided on the following pages.

In addition, you can also enroll in Cyberscout’s complimentary identity protection services by logging on to <https://bfs.cyberscout.com/activate> and following the instructions provided. When prompted, please provide the following unique code: [REDACTED]. In order for you to receive the monitoring services, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and an email account, and may not be available to minors under the age of 18. 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

For More Information. If you have any questions regarding the incident, please call 1-800-405-6108, Monday through Friday, between 8:00 am to 8:00 pm Eastern Time, excluding holidays.

The security of the information in our possession is a top priority for NewAgeSys. We take your trust in us and this matter very seriously, and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

NewAgeSys Inc.
4390 US-1, Suite 110
Princeton, NJ 08540

Steps You Can Take to Help 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 (the “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 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

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com/get-credit-report

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 www.annualcreditreport.com. For TransUnion: www.transunion.com/fraud-alerts.

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. For TransUnion: www.transunion.com/credit-freeze.

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
877-438-4338

California Attorney General

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

New York Attorney General

The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400



NC Attorney General

9001 Mail Service Center

Raleigh, NC 27699

ncdoj.gov/protectingconsumers/

877-566-7226

NY Bureau of Internet and Technology

28 Liberty Street

New York, NY 10005

www.dos.ny.gov/consumerprotection/

212.416.8433

Rhode Island: NewAgeSys is notifying 1,087 individuals of this incident.

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:

www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.