



Lindsey Smith, Partner
Constangy, Brooks, Smith & Prophete, LLP
Cybersecurity & Data Privacy Team
145 West Ostend Street, Suite 600
Baltimore, Maryland 21230
ldsmith@constangy.com
706.247.3613

March 28, 2025

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: ldtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP, represents Sunnking Sustainable Solutions (“Sunnking”), an electronics recycling and IT asset disposition services provider based in New York. Sunnking takes the protection of all information within its possession very seriously and has taken measures to reduce the likelihood of a similar incident reoccurring. This notice is being sent on behalf of Sunnking because personal information for 1 Maryland residents could have been involved in the data security incident.

1. Nature of the Security Incident

On February 5, 2025, we learned of unusual activity related in our network. In response, we took steps to investigate and learned that some data could have been viewed or downloaded without authorization. We then took steps to review the data that could have been involved. At the end of the review, on March 11, 2025, we took steps to locate the information needed to complete notification to the individuals involved.

The potentially affected information may have included individuals’ names and Social Security number.

2. Number of Maryland Residents Affected

Sunnking notified 1 Maryland residents within the potentially affected population on March 27, 2025, via USPS First-Class Mail. A sample copy of the notification letter sent to the potentially affected individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

As soon as Sunnking discovered the unusual network activity, we took steps to secure our systems and launched an investigation to learn more about what happened and what information could have been affected. We have implemented additional safeguards to enhance the security of our systems and to reduce the risk of a similar incident occurring in the future.

We have established a toll-free call center through Cyberscout, a TransUnion company, to answer questions about the incident and address related concerns. Additionally, we are providing notified individuals with complimentary access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services for 12 months.

4. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at 706.247.3613 or ldsmith@constangy.com.

Sincerely,

A handwritten signature in black ink, appearing to read 'Lindsey Smith', with a stylized flourish at the end.

Lindsey Smith
Partner, Constangy Cyber Team

Attachment: Sample Notification Letter



Sunnking Sustainable Solutions
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS554



[Redacted address block]



March 27, 2025

Subject: Notice of Data Security Incident

Dear [Redacted],

We are writing to inform you of a data security incident that may have involved your personal information. Sunnking Sustainable Solutions (“Sunnking”) is committed to maintaining our employees’ trust and demonstrating our commitment to data privacy and security. This letter has information about the incident and steps you can take to protect your information, including an opportunity to enroll in complimentary credit monitoring and identity protection services.

What happened? On February 5, 2025, Sunnking learned of unusual activity in our network. In response, we immediately took measures to terminate the activity and secure our systems. In addition, we engaged cybersecurity experts to investigate. Our investigation determined that certain data may have been accessed or downloaded without authorization. After a thorough review of the information, we determined that certain personal information was contained in the potentially affected data. We then took steps to locate the information needed to complete notification to the individuals involved. This process was completed on March 11, 2025.

What Information Was Involved? The information potentially impacted in connection with this incident varies for each individual, but may have included information such as your name and Social Security number.

What We Are Doing: As soon as we discovered the incident, we took the steps described above. We also performed a thorough review of our systems to investigate the incident and ensure that our systems remain secure. We also implemented additional security measures to protect our digital environment and minimize the likelihood of future incidents.

In addition, to help protect your information, we are offering you the opportunity to enroll in complimentary access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 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. Finally, 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.

What You Can Do: You can review the guidance included with this letter about how to protect your information. You can also contact our call center with any questions and to enroll in the free services 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: [REDACTED]. In order for you 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.

For More Information: If you have any questions about this letter, please contact our dedicated call center for this incident at 1-800-405-6108 toll-free Monday through Friday from 7:00 am – 7:00 pm Central time (excluding major U.S. holidays). Representatives are available for 90 days from the date of this letter, when you call, please supply the fraud specialist with your unique code listed above.

Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

Sunnking Sustainable Solutions
4 Owens Rd,
Brockport, NY 14420



Additional Steps You Can Take to Further Protect Your 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 1000
Chester, PA 19016
1-800-916-8800
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 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
877-438-4338

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

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

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

New York Attorney General
The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

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

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
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
202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

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.