



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

December 14, 2023

VIA EMAIL

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

Re: **Notice of Data Security Incident**

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP ("Constangy") represents Ascentia Real Estate Holding Company, LLC ("Ascentia") in connection with a recent data security incident described in greater detail below.

1. Nature of the Security Incident

On May 23, 2023, Ascentia discovered that it had experienced an incident disrupting access to certain of its systems. In response, Ascentia took immediate steps to secure its systems and promptly launched an investigation. In so doing, Ascentia engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization. On October 31, 2023, Ascentia learned that personal information for certain individuals may have been impacted, and began collecting up-to-date contact information for these individuals and arranged for notification letters to be sent as soon as possible.

2. Number of Affected Maryland Residents & Information Involved

The incident involved personal information for one (1) Maryland resident. The information involved for the impacted Maryland resident may have included name and Social Security number.

3. Notification to Affected Individuals

On December 14, 2023, notification letters were sent to the affected Maryland residents by USPS First Class Mail. The notification letter provides resources and steps these individuals can take to help protect their information. The notification letter also offers the individuals whose Social Security number was affected by this event the opportunity to enroll in 12 months of complimentary identity protection services, including credit monitoring, dark web monitoring, \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery

services. A sample notification letter sent to the impacted individual is included with this correspondence.

4. Steps Taken Relating to the Incident

In response to the incident, Ascentia retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. Ascentia also implemented additional security measures to further harden its digital environment in an effort to prevent a similar event from occurring in the future. Additionally, Ascentia reported the incident to the FBI and will cooperate with any resulting investigation.

Finally, Ascentia is notifying the affected individuals and providing them with steps they can take to protect their personal information as discussed above.

5. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at dmcmillan@constangy.com or 718.614.8371, or David Rice at or drice@constangy.com or 718.614.2656.

Best regards,

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

David McMillan of
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Enclosure: Sample Notification Letter

Ascentia Real Estate Holding Company, LLC
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-08181 1-1



December 14, 2023

Subject: Notice of Data Security Incident

Dear [REDACTED]

I am writing to inform you of a recent data security incident experienced by Ascentia Real Estate Holding Company, LLC (“Ascentia”) that may have affected your personal information. Ascentia takes the privacy and security of all information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened? On May 23, 2023, Ascentia discovered that it had experienced an incident disrupting access to certain of its systems. In response, Ascentia took immediate steps to secure its systems and promptly launched an investigation. In so doing, Ascentia engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization. On October 31, 2023, Ascentia learned that your personal information may have been impacted in connection with the incident which is the reason for this notification. Please note that Ascentia has no evidence of the misuse or attempted misuse of any potentially impacted information.

What Information Was Involved? The information potentially impacted in connection with this incident may have included your name as well as your Social Security number.

What Are We Doing? As soon as Ascentia discovered this incident, Ascentia took the steps described above. Ascentia also reported the incident to the FBI and will cooperate with any resulting investigation. In addition, Ascentia implemented measures to enhance the security of its digital environment in an effort to minimize the risk of a similar incident occurring in the future.

Although Ascentia has no evidence of the misuse of any potentially impacted information, Ascentia is 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. Finally, Ascentia is 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 through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

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

To enroll in the credit monitoring and identity protection services at no charge, please log on to <https://secure.identityforce.com/benefit/ascentia> 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: 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 1-833-966-0871 and supply the specialist with your unique code listed above.

Please accept my sincere apologies and know that Ascentia takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

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

Emily Patterson
VP of Finance and Accounting
Ascentia Real Estate Holding Company, LLC

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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the FTC is as follows:

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

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 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 can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 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 Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay 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. Additional information is available at <http://www.annualcreditreport.com>. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the FTC identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

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.

LCS Financial Services Contact Information: 6782 S. Potomac St., Centennial, CO 80112; 1.866.662.9087

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; [202-727-3400](tel:202-727-3400); oag@dc.gov

California: California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; <http://oag.ca.gov/>

Maine: Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; <https://www.maine.gov/ag/>

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>

Oregon: Oregon Office of the Attorney General can be reached at: Oregon Department of Justice, 1162 Court St. NE, Salem, OR, 97301, 1-877-877-9392, www.doj.state.or.us

Rhode Island: Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, <http://www.riag.ri.gov>. The total number of Rhode Island residents receiving notification of this incident is 0.

Texas: Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

Vermont: Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov