Laura K. Funk, Partner
Cybersecurity & Data Privacy Team
1201 Elm Street, Suite 2550
Dallas, Texas 75270
LFunk@constangy.com
Direct: 248.709.9385

November 4, 2024

VIA ELECTRONIC MAIL

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

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP represents Custom Wealth Management ("CWM"), a provider of financial advisory services based out of New York, in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland's data breach notification statute.

Nature of the Security Incident

On July 15, 2024, CWM became aware of suspicious activity in its email environment. In response, CWM immediately took steps to secure its environment and launched an investigation to determine whether sensitive or personal information may have been accessed or acquired during the incident. As a result of the investigation, CWM identified that the contents of one (1) employee mailbox may have been acquired without authorization. CWM then engaged an independent team to conduct a comprehensive review of all data within the employee mailbox, and on October 7, 2024, that review identified that the personal information associated with certain individual and corporate clients may have been affected. CWM then worked diligently to locate relevant address information and prepare the services being offered, which was completed on October 28, 2024.

The information affected varied between individuals but may have included name, address, date of birth, and Social Security number. Please note that we have no current evidence to suggest misuse or attempted misuse of personal information involved in the incident.

Number of Maryland Residents Involved

On November 4, 2024, CWM notified ten (10) Maryland residents of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

Steps Taken to Address the Incident

In response to the incident, CWM is providing individuals with information about steps that they can take to help protect their personal information, and, out of an abundance of caution, it is also offering individuals complimentary credit monitoring and identity protection services through IDX by Zerofox. This includes 12 months of credit and CyberScan dark web monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. Additionally, to help reduce the risk of a similar future incident, CWM has implemented additional technical security measures throughout the environment.

Contact Information

CWM 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 at LFunk@Constangy.com.

Sincerely,

Laura K. Funk
Partner
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Enclosure: Sample Notification Letter

P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code:<<XXXXXXXX>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip Code>>

November 4, 2024

Re: Notice of Data <<Variable Data 1>>

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a recent data security incident experienced by Custom Wealth Management ("CWM") that may have involved your personal information. At CWM, we take the privacy and security of all information within our possession very seriously. This is why we are notifying you of the incident, providing you with steps you can take to help protect your personal information, and offering you the opportunity to enroll in complimentary credit monitoring and identity protection services. While we have no conclusive evidence that your information was taken, even after extensive IT involvement, we are notifying you of the incident and providing you with the option to enroll in complimentary credit monitoring and identity protection services in accordance with industry requirements.

What Happened. On or around July 15, 2024, CWM became aware of suspicious activity in our email environment. We immediately took steps to ensure the security of our email tenant and launched an investigation to determine what happened and whether sensitive or personal information may have been accessed or acquired during the incident. As a result of the investigation, we identified that the contents of one individual's mailbox may have been accessed without authorization. CWM then engaged an independent team to conduct a comprehensive review of all potentially affected data within the mailbox, and on October 7, 2024, that review determined that the personal information associated with certain clients may have been affected. CWM then worked diligently to identify contact information to effectuate notification and prepare the services being offered to affected individuals, as provided in more detail below. This process was completed on October 28, 2024. There has been no conclusive evidence that your information was compromised but are nonetheless taking these steps for your protection.

What Information Was Involved. The information involved may have included your name, <<Variable Data 2>>. **Please note that we have no current evidence to suggest the misuse or attempted misuse of your personal information.**

What We Are Doing. As soon as CWM 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 are also providing you with information about steps you can take to help protect your personal information.

Additionally, we are offering you the opportunity to enroll in credit monitoring and identity protection services through IDX at no cost to you. The IDX services, which are free to you upon enrollment, include <<Membership Offering Length>> months of credit and CyberScan dark web monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do. Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information. In addition, we encourage you to enroll in the credit monitoring and identity

theft protection services we are offering through IDX at no cost to you. To receive credit monitoring 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.

You can enroll in the IDX identity protection services by calling 1-833-903-3648 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time. Please note the deadline to enroll is February 4, 2025.

For More Information. If you have questions about the incident, please call IDX at 1-833-903-3648, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time. IDX representatives are fully versed on this incident and can answer questions you may have regarding the protection of your personal information.

The team at CWM will continue to do all we can to ensure your information is safe and take whatever measures necessary to protect your information.

Sincerely,

Custom Wealth Management
7293 Buckley Road, Suite 100
Syracuse, NY 13212

STEPS YOU CAN TAKE TO HELP 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 (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

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 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, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

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.